И. Л. КАНТОР, А. С. СОЛОДОВНИКОВ

ГИПЕРКОМПЛЕКСНЫЕ ЧИСЛА

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1973

517.1
К 19
УДК 512.8

АННОТАЦИЯ

Эта брошюра посвящена гиперкомплексным числам — обобщению обычных комплексных чисел. В ней рассказывается о том, к чему приводит замена одной «мнимой единицы» i несколькими мнимыми единицами, иначе говоря, рассказывается о величинах вида $a + bi + cj \ldots$ В частности, книга знакомит читателя с замечательными примерами гиперкомплексных чисел — кватернионами и октавами. Эти числа играют большую роль в различных математических вопросах. В книге рассматриваются два таких вопроса: разыскание «алгебр с делением» (теорема Фробениуса) и разыскание «нормированных алгебр» (теорема Гурвица).

Исай Львович Кантор, Александр Самуилович Солодовников
ГИПЕРКОМПЛЕКСНЫЕ ЧИСЛА
М., 1973 г., 144 стр. с илл.

Редактор *В. В. Донченко*

Техн. редактор *Е. Н. Земская* Корректоры *О. А. Бутусова, А. Л. Ипатова*

Сдано в набор 17/VI 1973 г. Подписано к печати 11/XII 1973 г. Бумага 84×108¹/₃₂, тип. № 2. Физ. печ. л. 4,5. Услови. печ. л. 7,56. Уч.-изд. л. 6,93. Тираж 60 000 экз. Т-19920. Цена книги 22 коп. Заказ № 671

Издательство «Наука»
Главная редакция физико-математической литературы
117071, Москва, В-71, Ленинский проспект, 15

Ордена Трудового Красного Знамени
Ленинградская типография № 2 имени Евгении Соколовой
Союзполиграфпрома при Государственном комитете Совета Министров СССР
по делам издательств, полиграфии и книжной торговли,
198052, г. Ленинград, Измайловский проспект, 29

К $\frac{0223-1854}{042(02)-73}$ 82-73

ПРЕДИСЛОВИЕ

Предметом этой книжки являются различные системы «чисел», которые можно построить, исходя из действительных чисел, путем добавления ряда «мнимых единиц». Классический пример такой системы — это система комплексных чисел.

Одно из важнейших свойств комплексных чисел выражается тождеством

$$|zz'| = |z| \cdot |z'| \qquad (1)$$

(модуль произведения равен произведению модулей). Если обозначить $z = a_1 + a_2 i$, $z' = b_1 + b_2 i$, то (1) перепишется в виде

$$(a_1 b_1 - a_2 b_2)^2 + (a_1 b_2 + a_2 b_1)^2 = (a_1^2 + a_2^2)(b_1^2 + b_2^2).$$

Прочитанное справа налево, это тождество звучит так: «произведение суммы двух квадратов на сумму двух квадратов есть снова сумма двух квадратов».

Существуют ли подобные тождества с бо́льшим, чем 2, числом квадратов?

Как описать все такие тождества?

Еще Л. Эйлер указал пример тождества для 4 квадратов; позже было найдено тождество для 8 квадратов. Однако полное решение вопроса удалось получить только в конце XIX века.

Можно предположить, что каждое тождество «для n квадратов» связано с формулой (1), в которой z и z' обозначают уже не комплексные числа, а «числа» более общего вида:

$$a_1 + a_2 i + a_3 j + \ldots + a_n l,$$

где $i, j, \ldots, l$ — мнимые единицы. Несколько упрощая положение вещей, можно сказать, что это действительно

так. Установление связи между тождествами «для n квадратов» и формулой (1) для некоторых систем «гиперкомплексных» чисел составляет одну из основных линий в общем построении этой книжки.

Другой вопрос, которому уделено в этой книжке много места, — это вопрос о *делении* гиперкомплексных чисел. Дело в том, что в любой системе гиперкомплексных чисел определены только три из четырех «арифметических» операций: сложение, вычитание и умножение. Что же касается деления, то вопрос о возможности этой операции для данной системы гиперкомплексных чисел требует отдельного рассмотрения. Вообще, следует сказать, что гиперкомплексные системы, в которых возможно деление, составляют большую редкость. Разумеется, системы действительных чисел, так же как и комплексных, являются примерами систем с делением. Но, кроме них, имеются и другие примеры. Самыми замечательными среди них являются система так называемых *кватернионов* и система *октав*. Проблема разыскания *всех* гиперкомплексных систем с делением исчерпывающим образом не решена и до сих пор. Несколько вариантов этой проблемы будут рассмотрены в данной книжке.

Первая глава этой книги знакомит читателя с различными примерами гиперкомплексных чисел, в том числе с «кватернионами» и «октавами»; для тех и других справедлива формула (1), и те и другие составляют «систему с делением». Третья глава посвящена исключительной роли, которую играют три системы: комплексных чисел, кватернионов, октав по отношению к поставленным выше вопросам. Вторая глава является вспомогательной: в ней излагаются на элементарном уровне основные понятия линейной алгебры.

Книжка рассчитана на учащихся математических школ и просто всех интересующихся математикой. Первая и вторая главы в основном доступны школьнику старших классов, чтение других разделов может потребовать от него довольно напряженных усилий. Во всех случаях никаких предварительных знаний от читателя не требуется.

ГИПЕРКОМПЛЕКСНЫЕ ЧИСЛА

§ 1. Комплексные числа

1°. Вступление. В элементарной алгебре наряду с действительными числами рассматривается и более широкая система *комплексных* чисел. Причина, заставляющая рассматривать комплексные числа, связана с решением квадратных уравнений. Дело в том, что некоторые квадратные уравнения, например,

$$x^2 + 1 = 0, \tag{1}$$

нельзя решить, ограничиваясь только действительными числами (не существует такого действительного числа a, чтобы a^2 было равно -1).

История комплексных чисел начинается с XVI века. Итальянские математики Джироламо Кардано и Рафаэль Бомбелли, решая квадратные уравнения, ввели в рассмотрение символ $\sqrt{-1}$ — формальное решение уравнения (1), а также выражения $b\sqrt{-1}$ — формальные решения уравнений

$$x^2 + b^2 = 0.$$

Выражения более общего вида $a + b\sqrt{-1}$ можно рассматривать тогда как формальные решения уравнений

$$(x - a)^2 + b^2 = 0. \tag{2}$$

Впоследствии выражения $a + b\sqrt{-1}$ стали называться «мнимыми», а затем «комплексными» числами и записываться $a + bi$ (символ i для обозначения $\sqrt{-1}$ ввел Л. Эйлер в XVIII в.). Этих чисел оказывается уже достаточно для решения *любого* квадратного уравнения (если дискриминант квадратного уравнения неотрицателен, то, как известно, корни такого уравнения —

действительные числа, если же дискриминант отрицателен, то уравнение обязательно приводится к виду (2)).

Итак, комплексным числом называется выражение вида

$$a + bi,$$

где a и b — действительные числа, а символу i приписывается свойство $i^2 = -1$. Заметим, что среди комплексных чисел содержатся, в частности, все действительные числа (они получаются при $b = 0$), а также все «чисто мнимые» числа bi (они получаются при $a = 0$).

Обозначая для краткости комплексное число одной буквой z, будем дальше писать

$$z = a + bi.$$

Число a называется *действительной частью*, а число bi — *мнимой частью* комплексного числа z; сам символ i называют «мнимой единицей». Название «мнимая» не следует понимать буквально; оно сохранилось с тех времен (XVI—XVII вв.), когда комплексные числа считались чем-то нереальным и были окружены ореолом глубокой таинственности. Для теперешней математики комплексные числа — вещь совершенно естественная (не более «мнимая», чем сами действительные числа).

2°. Действия над комплексными числами. Сложение, вычитание и умножение комплексных чисел естественно определить следующим образом:

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

$$(a + bi) - (c + di) = (a - c) + (b - d)i,$$

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$$

(определяя умножение, мы учли тот факт, что $i^2 = -1$).

Отметим попутно, что если в равенстве, определяющем умножение комплексных чисел, положить $b = 0$, то получим правило умножения действительного числа на комплексное:

$$a(c + di) = ac + adi.$$

Нетрудно проверить, что законы, которым подчиняются определенные выше операции над комплексными числами, те же самые, что и законы действий над дей-

ствительными числами. Сложение обладает переместительным и сочетательным свойствами:

$$z_1 + z_2 = z_2 + z_1, \quad (z_1 + z_2) + z_3 = z_1 + (z_2 + z_3),$$

то же самое относится к умножению:

$$z_1 z_2 = z_2 z_1, \quad (z_1 z_2) z_3 = z_1 (z_2 z_3);$$

наконец, справедлив распределительный закон, устанавливающий связь между этими двумя действиями:

$$z_1 (z_2 + z_3) = z_1 z_2 + z_1 z_3. \tag{3}$$

Проверим, например, справедливость равенства (3). Пусть

$$z_1 = a_1 + b_1 i, \quad z_2 = a_2 + b_2 i, \quad z_3 = a_3 + b_3 i.$$

Имеем

$$z_1 (z_2 + z_3) = (a_1 + b_1 i)((a_2 + a_3) + (b_2 + b_3) i) =$$
$$= (a_1 (a_2 + a_3) - b_1 (b_2 + b_3)) + (a_1 (b_2 + b_3) + b_1 (a_2 + a_3)) i,$$
$$z_1 z_2 + z_1 z_3 = (a_1 + b_1 i)(a_2 + b_2 i) + (a_1 + b_1 i)(a_3 + b_3 i) =$$
$$= (a_1 a_2 - b_1 b_2 + a_1 a_3 - b_1 b_3) + (a_1 b_2 + b_1 a_2 + a_1 b_3 + b_1 a_3) i;$$

сравнивая результаты обоих вычислений, убеждаемся в том, что они совпадают.

3°. **Операция сопряжения.** Остановимся теперь на других свойствах системы комплексных чисел.

Каждому комплексному числу

$$z = a + bi$$

можно сопоставить другое комплексное число $a - bi$, которое называется *сопряженным* к z и обозначается $\bar{z}$. Таким образом, по определению,

$$\bar{z} = a - bi.$$

Легко убедиться, что справедливы формулы

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$$

и

$$\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2,$$

иначе говоря, сопряженное к сумме равно сумме сопряженных и сопряженное к произведению равно произведению сопряженных. Проверку этих формул мы предоставим читателю.

Складывая и перемножая числа z и $\bar{z}$, находим

$$z+\bar{z}=2a$$

и

$$z\bar{z}=a^2+b^2,$$

т. е. сумма и произведение сопряженных комплексных чисел всегда являются действительными числами.

4°. Модуль комплексного числа. Тождество для двух квадратов. Неотрицательное действительное число $\sqrt{a^2+b^2}$ называется *модулем* комплексного числа z и обозначается $|z|$:

$$|z|=\sqrt{a^2+b^2}.$$

Итак,

$$z\bar{z}=|z|^2.$$

Из последнего равенства вытекает одно замечательное следствие. Пусть z_1 и z_2 — два комплексных числа. Имеем

$$|z_1z_2|^2=(z_1z_2)\overline{(z_1z_2)}=z_1z_2\bar{z}_1\bar{z}_2=z_1\bar{z}_1\cdot z_2\bar{z}_2=|z_1|^2|z_2|^2,$$

следовательно,

$$|z_1z_2|^2=|z_1|^2|z_2|^2 \tag{4}$$

или

$$|z_1z_2|=|z_1||z_2|. \tag{5}$$

Таким образом, *модуль произведения равен произведению модулей.* Это — чрезвычайно важное свойство комплексных чисел; в § 16 ему будет присвоено специальное название (свойство *нормированности*). А сейчас посмотрим, как выглядит равенство (4) в подробной записи.

Если

$$z_1=a_1+b_1i, \qquad z_2=a_2+b_2i,$$

то

$$z_1z_2=(a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)\,i,$$

и равенство (4), записанное справа налево, принимает вид

$$(a_1^2+b_1^2)(a_2^2+b_2^2)=(a_1a_2-b_1b_2)^2+(a_1b_2+a_2b_1)^2.$$

Получилось довольно любопытное тождество. Допуская некоторую расплывчатость формулировки, его можно

прочитать так: *произведение суммы двух квадратов на сумму двух квадратов есть снова сумма двух квадратов.*

Естественно возникает вопрос: существуют ли аналогичные тождества с бóльшим числом квадратов? Вопрос, как мы дальше увидим, совсем не простой; в течение многих лет он занимал умы математиков. В настоящей книжке этому вопросу отводится одно из центральных мест. В § 3 мы сформулируем его более отчетливо, а в гл. 3 расскажем, как он решается.

5°. Деление комплексных чисел. До сих пор мы совсем не касались вопроса о *делении* комплексных чисел; поговорим об этом теперь.

Пусть z' и z — два комплексных числа, причем $z \neq 0$. Частное от деления z' на z есть, по определению, решение уравнения

$$zx = z'. \tag{6}$$

Умножив обе части уравнения на $\bar{z}$, получим $\bar{z}zx = \bar{z}z'$ или

$$|z|^2 x = \bar{z}z';$$

если теперь умножить обе части на действительное число $\frac{1}{|z|^2}$, то будем иметь

$$x = \frac{1}{|z|^2}\bar{z}z'. \tag{7}$$

В том, что найденное значение x действительно удовлетворяет уравнению (6), легко убедиться непосредственной проверкой.

Проиллюстрируем деление примером. Пусть требуется разделить $z' = 5 - i$ на $z = 2 - 3i$. По формуле (7) имеем

$$\frac{z'}{z} = \frac{1}{2^2 + 3^2}(2 + 3i)(5 - i) = \frac{1}{13}(13 + 13i) = 1 + i.$$

§ 2. Другие арифметики для чисел $a + bi$

1°. Постановка задачи. Итак, мы построили числовую систему из выражений вида $a + bi$, определив сложение и умножение таких выражений по формулам

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \tag{1}$$

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i. \tag{2}$$

Что касается формулы (1), то она представляется вполне естественной. Напротив, вид формулы (2) не вызывает такого ощущения. Посмотрим, нельзя ли из тех же выражений $a+bi$ получить достаточно разумную числовую систему, сохранив правило сложения (1), но заменив (2) *каким-либо новым* законом умножения.

Как мог бы выглядеть этот новый закон? В значительной мере это зависит от того, какими свойствами мы хотим наделить новое умножение. Скажем, было бы нелепо ввести его формулой

$$(a+bi)\cdot(c+di)=ac^2+bdi,$$

ибо тогда, например, при $b=0$, $d=0$ мы получили бы довольно странное равенство

$$a\cdot c=ac^2.$$

Укажем те требования, которые мы собираемся предъявить к новому умножению:

1) Умножение действительного числа a, рассматриваемого как элемент новой числовой системы ($a=a+0i$), на произвольное число $z=b+ci$ должно давать тот же результат, что и в случае комплексных чисел, т. е.

$$(a+0i)(b+ci)=ab+aci$$

и

$$(b+ci)(a+0i)=ab+aci.$$

В частности, это означает, что для действительных чисел новое умножение должно совпадать с обычным:

$$(a+0i)(b+0i)=ab+0i.$$

Поскольку то же самое верно и в отношении сложения (из (1) следует $(a+0i)+(b+0i)=(a+b)+0i$), то тем самым действительные числа включаются в новую числовую систему с их естественной арифметикой.

2) Должно выполняться равенство

$$(az_1)\cdot(bz_2)=(ab)\cdot(z_1z_2),$$

где a и b — любые действительные числа. Например, $(2i)(3i)=6i^2$.

3) Как для первого сомножителя, так и для второго должно выполняться свойство распределительности, связывающее умножение со сложением:

$$z_1(z_2 + z_3) = z_1z_2 + z_1z_3$$

и

$$(z_1 + z_2)z_3 = z_1z_3 + z_2z_3.$$

Конечно, эти требования еще не позволяют написать до конца новый закон умножения, но все же из них следует многое. А именно,

$$(a + bi)(c + di) = a(c + di) + (bi)(c + di) = \\ = ac + adi + bci + bdi^2.$$

Теперь, чтобы написать результат, остается только указать, чему равно i^2. Приняв $i^2 = -1$, приходим к умножению комплексных чисел. Но это — отнюдь не единственная возможность. В принципе ведь нужно лишь, чтобы произведение $i \cdot i$ принадлежало рассматриваемой нами системе чисел, т. е. было числом вида $p + qi$. Задав p и q, мы окончательно устанавливаем вид закона умножения:

$$(a + bi)(c + di) = (ac + bdp) + (ad + bc + bdq)i. \quad (3)$$

Предмет нашего изучения, таким образом, определился. Теперь можно забыть о «наводящих» соображениях, которые привели нас к формуле (3), и просто сказать, что *рассматривается система чисел вида* $a + bi$ *с законом сложения* (1) *и законом умножения* (3), *где* p *и* q *— два фиксированных действительных числа* (определяющих собой, так сказать, «арифметику» данной системы чисел).

Внимательно рассмотрев формулу (3), мы довольно легко убеждаемся, что новое умножение обладает переместительным свойством ($z_1z_2 = z_2z_1$) — довольно неожиданный результат, если учесть, что среди требований, предъявленных к умножению, такого свойства не было! Выполняется и сочетательное свойство ($(z_1z_2)z_3 = z_1(z_2z_3)$), хотя проверка этого факта требует несколько

большего терпения. Имеем

$$[(a+bi)(c+di)](e+fi) =$$
$$= [(ac+bdp)+(ad+bc+bdq)i](e+fi) =$$
$$= \underline{((ac+bdp)e+(ad+bc+bdq)fp)} +$$
$$+ \underline{\underline{((ac+bdp)f+(ad+bc+bdq)e}} +$$
$$+ \underline{\underline{(ad+bc+bdq)fq)i}},$$

$$(a+bi)[(c+di)(e+fi)] =$$
$$= (a+bi)[(ce+dfp)+(cf+de+dfq)i] =$$
$$= \underline{(a(ce+dfp)+b(cf+de+dfq)p)} +$$
$$+ \underline{\underline{(a(cf+de+dfq)+b(ce+dfp)+b(cf+de+dfq)q)i}};$$

сравнивая результаты обоих вычислений, легко убедиться в их тождественности (чтобы облегчить проверку, мы подчеркнули равные выражения одинаковым числом прямых линий).

2°. Сведение к трем системам. Может показаться, что мы нашли бесчисленное множество числовых систем, поскольку в формулу (3) входят два произвольных действительных числа p и q. Но это не совсем так. Сейчас мы увидим, что любая система сводится к одной из трех:

I) числа $a+bi$, где $i^2=-1$ (комплексные числа);

II) числа $a+bi$, где $i^2=1$ (так называемые *двойные числа*);

III) числа $a+bi$, где $i^2=0$ (так называемые *дуальные числа*).

Сведение любого случая к одному из этих трех осуществляется следующим образом.

Из равенства $i^2=p+qi$ вытекает $i^2-qi=p$ или:

$$\left(i-\frac{q}{2}\right)^2=p+\frac{q^2}{4}. \qquad (4)$$

Возможны три случая:

I. $p+\frac{q^2}{4}$ — отрицательное число, т. е. $p+\frac{q^2}{4}=-k^2$, где k — некоторое отличное от нуля действительное число. Тогда

$$\left(i-\frac{q}{2}\right)^2=-k^2,$$

т. е.

$$\left(-\frac{q}{2k}+\frac{1}{k}i\right)^2=-1. \qquad (5)$$

Обозначив число, стоящее в скобках, через J, будем иметь:

$$J^2 = -1.$$

При этом $i = \frac{q}{2} + kJ$, так что любое число $a + bi$ может быть записано в виде

$$a + bi = a + b\left(\frac{q}{2} + kJ\right) = \left(a + \frac{b}{2}q\right) + bkJ;$$

иначе говоря, число $a + bi$ допускает представление в виде $a' + b'J$, где $J^2 = -1$. Это означает, что *фактически мы имеем дело с комплексными числами.*

II. $p + \frac{q^2}{4}$ — положительное число, т. е. $p + \frac{q^2}{4} = k^2$ ($k \neq 0$). Тогда вместо (5) получим

$$\left(-\frac{q}{2k} + \frac{1}{k}i\right)^2 = 1.$$

Обозначив на этот раз число, стоящее в скобках, через E, будем иметь

$$E^2 = 1.$$

Таким образом, любое число $a + bi$ нашей системы допускает представление в виде $a' + b'E$, но теперь $E^2 = 1$. Закон умножения таких чисел будет

$$(a' + b'E)(c' + d'E) = (a'c' + b'd') + (a'd' + b'c')E.$$

Итак, при $p + \frac{q^2}{4} > 0$ *получаем систему двойных чисел.*

III. $p + \frac{q^2}{4} = 0$. В этом случае, обозначив через Ω число $i - \frac{q}{2}$, будем иметь

$$\Omega^2 = 0.$$

Любое число $a + bi$ нашей системы может быть переписано в виде $\left(a + \frac{b}{2}q\right) + b\Omega$, т. е. в виде $\tilde{a} + \tilde{b}\Omega$. Закон умножения выглядит так:

$$(\tilde{a} + \tilde{b}\Omega)(\tilde{c} + \tilde{d}\Omega) = \tilde{a}\tilde{c} + (\tilde{a}\tilde{d} + \tilde{b}\tilde{c})\Omega.$$

Это — система дуальных чисел.

Подведем итог. Мы показали, что *любая система чисел* $a+bi$ *с правилами действий* (1), (3) *фактически есть одна из трех*:

I) *комплексные числа* $a+bJ$, $J^2=-1$;

II) *двойные числа* $a+bE$, $E^2=1$;

III) *дуальные числа* $a+b\Omega$, $\Omega^2=0$.

Свойства комплексных чисел мы изучили достаточно детально. Дуальные и двойные числа менее интересны. Главное их отличие от комплексных чисел заключается в том, что дуальные числа, так же как и двойные, вообще говоря, *нельзя делить друг на друга.* Впрочем, здесь необходимо еще раз объяснить смысл слова «деление». Если задан некоторый закон умножения, то разделить z_1 на z_2 ($z_2\neq 0$) означает решить уравнение

$$z_2x=z_1.$$

Покажем, что в системе двойных чисел невозможно, например, разделить число $z_1=1$ (т. е. $1+0E$) на $z_2=1+E$. Действительно, если бы уравнение

$$(1+E)x=1+0E$$

имело решение, то, умножив обе части равенства на $1-E$, мы получили бы $(1-E^2)x=1-E$, т. е. $0=1-E$ — неверное равенство.

Точно так же в системе дуальных чисел нельзя, например, разделить 1 на Ω. Действительно, для любого $x=a+b\Omega$ имеем $x\cdot\Omega=a\Omega\neq 1$.

Конечно, невозможность деления ставит под сомнение право двойных и дуальных чисел называться «числами»: ведь главное в понятии числа именно в том и состоит, что числа можно складывать, вычитать, умножать и делить. Однако в математике играют большую роль и такие системы «чисел» (подобных двойным и дуальным), где определены лишь действия сложения, вычитания и умножения, в то время как деление выполняется не всегда (т. е. не для всех z_1, $z_2\neq 0$). В тех же случаях, когда деление выполняется для любых z_1, $z_2\neq 0$, говорят о *системе с делением.* В этой книжке мы будем, в основном, рассматривать системы с делением.

§ 3. Кватернионы

1°. Предварительные соображения. Опыт построения системы комплексных (а также двойных и дуальных) чисел наводит на мысль пойти дальше и рассмотреть числа вида

$$z = a + bi + cj,$$

где a, b, c — произвольные действительные числа, а i и j — некоторые символы. В качестве правила сложения для чисел такого вида, по-видимому, разумно принять

$$(a + bi + cj) + (a' + b'i + c'j) = \\ = (a + a') + (b + b')\,i + (c + c')\,j,$$

что же касается правила умножения, то над ним приходится задуматься. От этого правила мы хотели бы, разумеется, чтобы оно не приводило к слишком странным последствиям; например, желательно, чтобы для действительных чисел новое умножение совпадало с обычным:

$$(a + 0i + 0j)(b + 0i + 0j) = ab + 0i + 0j.$$

В предыдущем параграфе были перечислены те требования естественного характера, которые предъявляются к новому умножению. Повторим их снова:

1) Произведение действительного числа $k = k + 0i + 0j$ на произвольное число $z = a + bi + cj$ должно равняться $ka + kbi + kcj$.

2) Должно выполняться равенство

$$(az_1)(bz_2) = (ab)(z_1z_2),$$

где a и b — произвольные действительные числа.

3) Должен выполняться распределительный закон как в форме

$$z_1(z_2 + z_3) = z_1z_2 + z_1z_3,$$

так и в форме

$$(z_1 + z_2)z_3 = z_1z_3 + z_2z_3.$$

Придумать закон умножения, удовлетворяющий всем перечисленным требованиям, не составляет труда. Можно, например, принять

$$(a + bi + cj)(a' + b'i + c'j) = \\ = aa' + (ab' + ba')\,i + (ac' + ca')\,j;$$

при таком правиле умножения выполняются даже переместительный и сочетательный законы ($z_1z_2 = z_2z_1$ и $(z_1z_2)z_3 = z_1(z_2z_3)$), но что определенно отсутствует — так это возможность деления! Например, нельзя разделить 1 на i: уравнение

$$(0 + 1i + 0j)\,x = 1 + 0i + 0j$$

не имеет решения.

И это не случайно. Можно показать, что при любом правиле умножения чисел $a + bi + cj$, удовлетворяющем условиям 1), 2), 3), найдется хотя бы одна пара чисел z_1, z_2 (причем $z_2 \neq 0$) таких, что z_1 *нельзя разделить на* z_2. Таким образом, из чисел вида $a + bi + cj$ построить систему с делением невозможно!

Однако оказывается, что если присоединить еще один символ k и рассмотреть числа вида

$$a + bi + cj + dk, \tag{1}$$

то можно получить систему с делением. Говоря более точно, можно так ввести умножение для чисел (1), чтобы, помимо требований 1), 2), 3), выполнялось еще и обратное для умножения действие — деление. Наиболее интересным примером такой системы являются *кватернионы* («четверные» числа).

2°. Определение кватернионов. Так называются числа вида (1) с законом сложения

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) =$$
$$= (a + a') + (b + b')\,i + (c + c')\,j + (d + d')\,k$$

и весьма своеобразным законом умножения. Чтобы описать этот закон, достаточно указать, чему равны всевозможные парные произведения чисел i, j, k. Положим, по определению,

$$\begin{aligned} i^2 &= -1, \quad j^2 = -1, \quad k^2 = -1, \\ ij &= k, \quad ji = -k, \\ jk &= i, \quad kj = -i, \\ ki &= j, \quad ik = -j. \end{aligned} \tag{2}$$

Запомнить эту «таблицу умножения» помогает рис. 1, на котором кватернионы i, j, k изображены тремя точ-

ками окружности, расположенными по направлению движения часовой стрелки. Произведение любых двух чисел из тройки i, j, k равно третьему, если движение от первого множителя ко второму происходит по часовой стрелке, и равно третьему со знаком минус, если движение происходит против часовой стрелки. Как видим, переместительное свойство умножения здесь не выполняется: произведение зависит от порядка сомножителей!

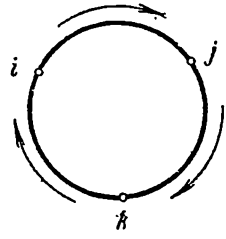


Рис. 1.

Умножение произвольных кватернионов производится с помощью приведенной выше таблицы и с учетом требований 1) —3). Пусть

$$q = a + bi + cj + dk,$$
$$q' = a' + b'i + c'j + d'k.$$

По правилу умножения суммы на сумму (вытекающему из 3)), имеем

$$qq' = aa' + a(b'i) + a(c'j) + a(d'k) + (bi)a' + (bi)(b'i) + (bi)(c'j) + (bi)(d'k) + (cj)a' + (cj)(b'i) + (cj)(c'j) + (cj)(d'k) + (dk)a' + (dk)(b'i) + (dk)(c'j) + (dk)(d'k).$$

Мы получили сумму 16 слагаемых. Преобразуя каждое из них с помощью требований 1), 2) и таблицы умножения (например, $(bi)(c'j) = bc'(ij) = bc'k$), приходим к результату:

$$qq' = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i + (ac' + ca' + db' - bd')j + (ad' + da' + bc' - cb')k. \quad (3)$$

3°. Сочетательный закон для умножения кватернионов. Хотя умножение кватернионов не подчиняется переместительному закону, все же вычисления с кватернионами не столь трудны, как может показаться с первого взгляда. Дело в том, что *для умножения кватернионов выполняется сочетательный закон*:

$$(q_1q_2)q_3 = q_1(q_2q_3). \quad (4)$$

Проверим справедливость этого равенства.

Поскольку каждый кватернион q_α ($\alpha = 1, 2, 3$) представляет собой сумму четырех слагаемых ($q_\alpha = a_\alpha +$

$+ b_\alpha j + c_\alpha j + d_\alpha k)$, то левая часть (4) равна сумме $4 \times 4 \times 4 = 64$ слагаемых вида

$$(u_1 u_2) u_3, \tag{5}$$

где u_1 — любое из четырех слагаемых кватерниона q_1, u_2 — любое из слагаемых для q_2, u_3 — любое слагаемое для q_3. Аналогично, правая часть (4) равна сумме 64 соответствующих слагаемых

$$u_1 (u_2 u_3). \tag{6}$$

Поэтому, если мы докажем, что каждое слагаемое (5) равно соответствующему слагаемому (6), то этим равенство (4) будет доказано.

Итак, все сводится к проверке равенства (4), когда в качестве q_1, q_2, q_3 фигурируют (в любой комбинации) кватернионы вида a, bi, cj, dk. При этом, так как числовой множитель можно выносить за знак произведения, то равенство (4) достаточно проверить для случаев, когда q_1, q_2, q_3 — это любые из кватернионов 1, i, j, k; например, вместо

$$((bi)(cj))(b'i) = (bi)((cj)(b'i))$$

достаточно доказать

$$(ij) i = i (ji).$$

В тех случаях, когда один из кватернионов q_1, q_2, q_3 равен 1, равенство (4) очевидно. Поэтому задача сводится к проверке этого равенства для случаев, когда q_1, q_2, q_3 — любые из кватернионов i, j, k.

Всего, таким образом, подлежат проверке 27 равенств. Выпишем для примера некоторые из них:

$$(ii) i = i (ii), \quad (ii) j = i (ij), \quad (ij) i = i (ji), \quad (ij) k = i (jk).$$

Справедливость каждого из 27 равенств легко следует из таблицы умножения (2).

Итак, умножение кватернионов обладает сочетательным свойством.

Ниже мы увидим, что система кватернионов во многих важнейших отношениях подобна системе комплексных чисел. Только что мы убедились в сочетательности умножения кватернионов. Однако близость кватернионов и комплексных чисел простирается значительно дальше. Во-первых, как уже упоминалось, для кватер-

нионов возможно деление. Во-вторых, можно естественным образом ввести для кватернионов понятие модуля так, чтобы выполнялось правило «модуль произведения равен произведению модулей».

В основе указанной близости лежит наличие в системе кватернионов операции сопряжения, обладающей сходными свойствами с сопряжением комплексных чисел.

4°. Сопряжение кватернионов. По аналогии с комплексными числами введем такое определение.

Пусть дан кватернион

$$q = a + bi + cj + dk.$$

Сопряженным ему называется кватернион

$$\bar{q} = a - bi - cj - dk. \tag{7}$$

Очевидно, что сумма сопряженных кватернионов есть число действительное. Но и произведение $q\bar{q}$ также является действительным числом, что сразу же следует из формулы (3) для умножения:

$$(a+bi+cj+dk)(a-bi-cj-dk) = a^2 + b^2 + c^2 + d^2. \tag{8}$$

Продолжая аналогию с комплексными числами, назовем число

$$\sqrt{a^2 + b^2 + c^2 + d^2}$$

модулем кватерниона q и условимся обозначать его $|q|$. Тогда последнее равенство перепишется так:

$$q\bar{q} = |q|^2$$

— в точности та же формула, что для комплексных чисел.

Замечание. Если q' есть «чисто мнимый» кватернион,

$$q' = bi + cj + dk,$$

то из формулы (8) следует

$$q'^2 = -(b^2 + c^2 + d^2) \leqslant 0.$$

Обратно, если квадрат некоторого кватерниона есть действительное число, меньшее или равное нулю, то

этот кватернион — чисто мнимый *). Таким образом, кватернионы $bi + cj + dk$, и только они, могут быть охарактеризованы условием, что их квадраты представляют собой действительные числа $\leqslant 0$. Учитывая это, можно дать другое описание операции сопряжения: *для произвольного кватерниона q берется его единственное представление в виде $a + q'$, где q' — кватернион, квадрат которого есть действительное число $\leqslant 0$, тогда* $\bar{q} = a - q'$. Это замечание нам пригодится впоследствии в § 17.

Непосредственная проверка показывает, что операция сопряжения обладает такими свойствами:

$$\overline{q_1 + q_2} = \bar{q}_1 + \bar{q}_2 \tag{9}$$

(сопряженное к сумме равно сумме сопряженных) и

$$\overline{q_1 q_2} = \bar{q}_2 \bar{q}_1 \tag{10}$$

(сопряженное к произведению равно произведению сопряженных, взятых в обратном порядке). Такие же равенства, как помнит читатель, справедливы и в случае комплексных чисел; нужно только иметь в виду, что для комплексных чисел вместо $\bar{z}_2\bar{z}_1$ можно писать $\bar{z}_1\bar{z}_2$ (ибо произведение не зависит от порядка сомножителей), в то время как для кватернионов, вообще говоря, $\bar{q}_2\bar{q}_1$ не равно $\bar{q}_1\bar{q}_2$.

Чтобы убедиться в справедливости равенства (10), достаточно проверить его для каждого из случаев, когда вместо q_1 и q_2 берутся i, j, k. Проверка легко осуществляется с помощью таблицы (2). Например,

$$\overline{ii} = \overline{-1} = -1, \quad \text{но и} \quad \bar{i}\bar{i} = (-i)(-i) = i^2 = -1,$$

$$\overline{ij} = \bar{k} = -k, \quad \text{но и} \quad \bar{j}\bar{i} = (-j)(-i) = ji = -k$$

и т. д.

5°. **Выполнимость деления в системе кватернионов.** Прежде всего обратим внимание на существенное отличие в самой постановке вопросов о делении кватернионов и делении комплексных чисел. Для комплексных

*) Действительно, для кватерниона $q = a + bi + cj + dk$ имеем $q^2 = (a + q')(a + q') = a^2 + q'^2 + 2aq' = a^2 - b^2 - c^2 - d^2 + 2aq'$.

Если это выражение является действительным числом и $a \neq 0$, то $q' = 0$; но тогда $q = a$ и, следовательно, q^2 не может быть $\leqslant 0$.

чисел, как помнит читатель, частным от деления z_1 на z_2 называется решение уравнения $z_2 x = z_1$. Но для кватернионов произведение зависит от порядка сомножителей, поэтому вместо одного уравнения нужно рассматривать два:

$$q_2 x = q_1 \tag{11}$$

и

$$x q_2 = q_1. \tag{11'}$$

Соответственно этому решение первого уравнения будем называть *левым частным* от деления q_1 на q_2 и обозначать $x_л$, а решение второго — правым частным $x_п$ (в случае комплексных чисел оба частных, очевидно, совпадают).

Чтобы решить уравнения (11) и (11'), применим тот же самый прием, что и в случае комплексных чисел. Умножим обе части уравнения (11) слева сначала на $\bar{q}_2$, а затем на $\frac{1}{|q_2|^2}$. Получим

$$x = \frac{1}{|q_2|^2} \bar{q}_2 q_1.$$

Непосредственной подстановкой в уравнение (11) убеждаемся, что это выражение действительно является решением. Таким образом,

$$x_л = \frac{1}{|q_2|^2} \bar{q}_2 q_1.$$

Аналогично находится $x_п$:

$$x_п = \frac{1}{|q_2|^2} q_1 \bar{q}_2.$$

В качестве примера найдем левые и правые частные от деления k на $1 + i + k$:

$$x_л = \frac{1}{3}(1 - i - k)\, k = \frac{1}{3}(k + j + 1),$$

$$x_п = \frac{1}{3} k\, (1 - i - k) = \frac{1}{3}(k - j + 1).$$

Итак, мы установили два наиболее важных свойства системы кватернионов:

1) для умножения кватернионов справедлив сочетательный закон;

2) кватернионы — система с делением.

6°. Модуль произведения. Еще одно важное свойство кватернионов состоит в том, что *модуль произведения равен произведению модулей.* Доказательство в точности такое же, как и в случае комплексных чисел; в нем используется формула $\overline{q_1q_2} = \bar{q}_2\bar{q}_1$ и свойство сочетательности для умножения кватернионов. Вот это доказательство:

$$|q_1q_2|^2 = (q_1q_2)\overline{(q_1q_2)} = (q_1q_2)(\bar{q}_2\bar{q}_1) = q_1(q_2\bar{q}_2)\bar{q}_1 = |q_1|^2|q_2|^2.$$

7°. Тождество для четырех квадратов. Общая постановка задачи о сумме квадратов. Полученное нами равенство

$$|q_1q_2|^2 = |q_1|^2|q_2|^2, \tag{12}$$

если записать его подробно, приводит к интересному тождеству. Пусть

$$q_1 = a + bi + cj + dk, \qquad q_2 = a' + b'i + c'j + d'k;$$

тогда q_1q_2 есть выражение, стоящее в правой части равенства (3). Следовательно, формула (12), читаемая справа налево, принимает вид

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2) = \\ = (aa' - bb' - cc' - dd')^2 + (ab' + ba' + cd' - dc')^2 + \\ + (ac' + ca' + db' - bd')^2 + (ad' + da' + bc' - cb')^2. \end{aligned} \tag{13}$$

Напомним, что в случае комплексных чисел равенство $|z_1z_2|^2 = |z_1|^2|z_2|^2$ привело нас к аналогичному тождеству

$$(a^2 + b^2)(a'^2 + b'^2) = (aa' - bb')^2 + (ab' + ba')^2, \tag{14}$$

которому мы дали такое истолкование: произведение суммы двух квадратов на сумму двух квадратов есть снова сумма двух квадратов. Аналогичное истолкование допускает, очевидно, и тождество (13): *произведение суммы четырех квадратов на сумму четырех квадратов есть снова сумма четырех квадратов.*

Отвлекаясь от комплексных чисел и кватернионов, естественно поставить теперь такой вопрос: для каких n найдется тождество «произведение суммы n квадратов на сумму n квадратов равно сумме n квадратов»?

При $n = 1$ решение приходит сразу:

$$a^2b^2 = (ab)^2,$$

но это слишком просто. При $n = 2$ и $n = 4$ ответ, как мы видим, тоже является положительным — это заранее совсем не очевидно! А как обстоит дело с $n = 3$? С $n = 5$, 6 и т. д.? Как уже отмечалось, этот вопрос долгое время не получал окончательного решения. Исчерпывающий ответ был получен в 1898 г. немецким математиком А. Гурвицем, который доказал удивительную теорему: тождества интересующего нас типа *возможны только при* $n = 1, 2, 4, 8$ и невозможны ни при каких других n.

Чтобы у читателя не оставалось никакой неясности в постановке «задачи о сумме квадратов», сформулируем ее сейчас более точно.

Пусть $a_1, a_2, \ldots, a_n$ и $b_1, b_2, \ldots, b_n$ — два ряда букв. Назовем *формой второй степени* от этих букв любую сумму, слагаемые которой устроены следующим образом: каждое из них есть произведение одной из букв первого ряда на одну из букв второго, взятое с численным множителем. Например, выражение

$$a_1b_1 + 8a_1b_2 - 2a_3b_5 + 3a_3b_n$$

есть форма второй степени. Точная постановка «задачи о сумме квадратов» состоит в следующем. Требуется ответить: *каким должно быть число* n *и как должны быть выбраны* n *форм второй степени — обозначим их для краткости* $\Phi_1, \Phi_2, \ldots, \Phi_n$ — для того, чтобы было справедливо тождество

$$(a_1^2 + a_2^2 + \ldots + a_n^2)(b_1^2 + b_2^2 + \ldots + b_n^2) = \\ = \Phi_1^2 + \Phi_2^2 + \ldots + \Phi_n^2. \quad (1)$$

Обнаруженные нами ранее тождества для комплексных чисел и кватернионов, очевидно, были именно такого типа. Для комплексных чисел:

$$(a_1^2 + a_2^2)(b_1^2 + b_2^2) = (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2$$

и для кватернионов:

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = \\ = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 + \\ + (a_1b_3 + a_3b_1 + a_4b_2 - a_2b_4)^2 + (a_1b_4 + a_4b_1 + a_2b_3 - a_3b_2)^2$$

(в соответствии с общей постановкой задачи мы изменили обозначения в тождествах (13) и (14)).

В § 6 на базе еще одной системы чисел (так называемых октав) мы построим тождество (!) для $n = 8$. Таким образом, перечень значений n в тождестве (!) включает числа 1, 2, 4, 8. Упомянутая выше теорема Гурвица, утверждающая, что другие значения n невозможны, будет доказана в гл. 3 после того, как мы ознакомимся со всеми необходимыми для этого фактами.

§ 4. Кватернионы и векторная алгебра

Открытие кватернионов в середине XIX века дало толчок разнообразным исследованиям в области математики и физики. В частности, благодаря кватернионам возникла чрезвычайно плодотворная область математики — *векторная алгебра*. О связи, которая существует между исчислением кватернионов и операциями над векторами в трехмерном пространстве, мы расскажем в этом параграфе.

1°. Числовая и векторная части кватерниона. Напомним читателю некоторые положения, известные из геометрии. Если ввести в обычном пространстве прямоугольную систему координат и обозначить через i, j, k векторы длины 1, выходящие из начала координат и направленные вдоль координатных осей (рис. 2), то любая сумма вида

$$bi + cj + dk,$$

где b, c, d — действительные числа, будет представлять собой некоторый вектор. Этот вектор идет из начала координат O в точку M с координатами b, c, d.

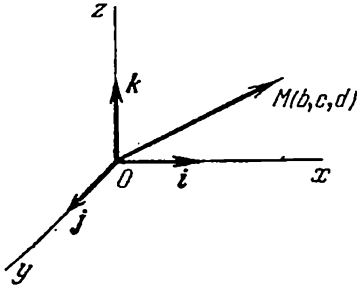


Рис. 2.

Возвращаясь к кватернионам, заметим, что каждый кватернион

$$q = a + bi + cj + dk$$

представляет собой формально сумму действительного числа a с вектором $bi + cj + dk$. Число a мы будем называть *числовой* (или *действительной*) частью, а выражение $bi + cj + dk$ — *векторной* (или *мнимой*) частью кватерниона q.

Рассмотрим теперь два чисто векторных кватерниона

$$q_1 = b_1 i + c_1 j + d_1 k \quad \text{и} \quad q_2 = b_2 i + c_2 j + d_2 k.$$

Перемножая их по правилу умножения кватернионов, будем иметь

$$q_1 q_2 = -(b_1 b_2 + c_1 c_2 + d_1 d_2) + (c_1 d_2 - d_1 c_2)\, i + (d_1 b_2 - b_1 d_2)\, j + (b_1 c_2 - c_1 b_2)\, k. \qquad (1)$$

Выпишем по отдельности числовую и векторную части кватерниона $q_1 q_2$.

$$\text{Числ. часть } q_1 q_2 = -(b_1 b_2 + c_1 c_2 + d_1 d_2). \qquad (2)$$

$$\text{Вект. часть } q_1 q_2 = (c_1 d_2 - d_1 c_2)\, i + (d_1 b_2 - b_1 d_2)\, j + (b_1 c_2 - c_1 b_2)\, k. \qquad (3)$$

2°. **Скалярное произведение.** Каждое из выражений (2), (3) имеет определенный геометрический смысл. Сумма $b_1b_2 + c_1c_2 + d_1d_2$, как мы сейчас покажем, равна $|q_1||q_2|\cos\varphi$, т. е. произведению длин векторов q_1 и q_2 (или, что то же, модулей кватернионов q_1 и q_2) на косинус угла между ними. Такое произведение приходится рассматривать в математике чрезвычайно часто; оно носит специальное название «скалярное произведение векторов q_1 и q_2» (подчеркнем, что скалярное произведение есть число, а не вектор) и обозначается обычно (q_1, q_2). Таким образом, по определению,

$$(q_1, q_2) = |q_1||q_2|\cos\varphi;$$

мы же хотим доказать формулу

$$(q_1, q_2) = b_1b_2 + c_1c_2 + d_1d_2. \quad (4)$$

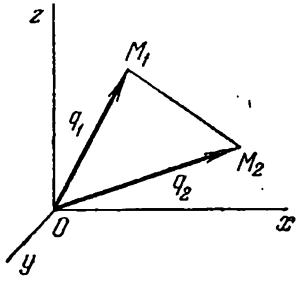


Рис. 3.

На рис. 3 изображен треугольник, построенный на векторах q_1 и q_2. Одна его вершина находится в начале координат, две другие вершины — точки M_1 и M_2 (концы векторов q_1 и q_2), координаты которых равны соответственно b_1, c_1, d_1 и b_2, c_2, d_2. Имеем

$$OM_1^2 = b_1^2 + c_1^2 + d_1^2,$$

$$OM_2^2 = b_2^2 + c_2^2 + d_2^2,$$

$$M_1M_2^2 = (b_1 - b_2)^2 + (c_1 - c_2)^2 + (d_1 - d_2)^2,$$

откуда

$$M_1M_2^2 = OM_1^2 + OM_2^2 - 2(b_1b_2 + c_1c_2 + d_1d_2).$$

Но по известной теореме косинусов

$$M_1M_2^2 = OM_1^2 + OM_2^2 - 2OM_1 \cdot OM_2 \cdot \cos\varphi,$$

где φ — угол при вершине O (угол между векторами q_1 и q_2). Сравнивая написанные равенства, получаем

$$OM_1 \cdot OM_2 \cdot \cos\varphi = b_1b_2 + c_1c_2 + d_1d_2,$$

что и требовалось доказать.

Итак, действительная часть произведения векторных кватернионов q_1 и q_2 равна взятому со знаком минус скалярному произведению q_1 на q_2.

Заметим, что если векторы q_1 и q_2 перпендикулярны, то их скалярное произведение равно нулю $\left(\varphi = \frac{\pi}{2},\ \cos\varphi = 0\right)$, следовательно, равна нулю и действительная часть произведения q_1q_2. В этом случае q_1q_2 будет «чистым» вектором. Обратное, конечно, тоже верно: если q_1q_2 — «чистый» вектор, то скалярное произведение

q_1 на q_2 равно нулю, значит, $\cos\varphi = 0$, и векторы q_1, q_2 перпендикулярны. Стоит еще заметить, что в случае, когда q_1 и q_2 перпендикулярны, $q_1q_2 = -q_2q_1$; это сразу же видно из формулы (1), если учесть, что действительная часть q_1q_2 равна нулю.

3°. Векторное произведение. Что касается векторной части произведения $\widetilde{q_1q_2}$, т. е. выражения, стоящего в правой части равенства (3), то установить ее геометрический смысл несколько труднее. Это выражение называют *векторным произведением* вектора q_1 на q_2 и обозначают $[q_1, q_2]$:

$$[q_1, q_2] = (c_1d_2 - d_1c_2)\,i + (d_1b_2 - b_1d_2)\,j + (b_1c_2 - c_1b_2)\,k.$$

Оказывается, вектор $[q_1, q_2]$ перпендикулярен каждому из векторов q_1 и q_2, а длина его равна $|q_1||q_2|\sin\varphi$ или, что то же, — площади S параллелограмма, построенного на векторах q_1 и q_2.

Чтобы доказать перпендикулярность векторов $[q_1, q_2]$ и q_1, достаточно, как мы знаем, проверить, что действительная часть произведения этих кватернионов равна нулю, или что их произведение является «чистым» вектором. Но в силу (1) и (4) имеем $[q_1, q_2] = q_1q_2 + (q_1, q_2)$, поэтому

$$q_1[q_1, q_2] = q_1(q_1q_2 + (q_1, q_2)) = q_1^2q_2 + (q_1, q_2)\,q_1 = -|q_1|^2 q_2 + (q_1, q_2)\,q_1\ ^*).$$

Справа получилась сумма двух векторов, т. е. снова вектор.

Перпендикулярность векторов $[q_1, q_2]$ и q_2 доказывается аналогично.

Найдем теперь длину вектора $[q_1, q_2]$. Квадрат ее равен

$$(c_1d_2 - d_1c_2)^2 + (d_1b_2 - b_1d_2)^2 + (b_1c_2 - c_1b_2)^2$$

или (после тождественных преобразований)

$$\left(b_1^2 + c_1^2 + d_1^2\right)\left(b_2^2 + c_2^2 + d_2^2\right) - \left(b_1b_2 + c_1c_2 + d_1d_2\right)^2.$$

Последнее выражение есть $|q_1|^2|q_2|^2 - (q_1, q_2)^2$ или, если вспомнить определение скалярного произведения,

$$|q_1|^2|q_2|^2 - |q_1|^2|q_2|^2\cos^2\varphi, \quad \text{т. е.} \quad |q_1|^2|q_2|^2\sin^2\varphi.$$

Итак, квадрат длины вектора $[q_1, q_2]$ равен $|q_1|^2|q_2|^2\sin^2\varphi$, т. е. S^2, что и требовалось доказать.

Обнаруженные нами свойства вектора $[q_1, q_2]$: перпендикулярность к q_1 и q_2, а также равенство его длины S — еще не определяют его полностью; такими свойствами обладают *ровно два* взаимно противоположных вектора (рис. 4). Какой же из них есть $[q_1, q_2]$? Последний штрих, завершающий описание вектора $[q_1, q_2]$, заключается в следующем: векторы q_1, q_2, $[q_1, q_2]$ ориентированы в пространстве подобно i, j, k.

---

*) В процессе вычислений мы заменили q_1^2 числом $-|q_1|^2$. Это можно сделать в силу формулы (1): из этой формулы следует

$$q_1^2 = -\left(b_1^2 + c_1^2 + d_1^2\right) + 0i + 0j + 0k = -|q_1|^2.$$

Этим мы хотим сказать, что если смотреть из конца вектора $[q_1, q_2]$ на плоскость векторов q_1 и q_2, то поворот на наименьший угол от q_1 к q_2 будет представляться происходящим в том же самом направлении (т. е. по направлению часовой стрелки или против), в каком из конца вектора k видится поворот на наименьший угол от i к j (рис. 5) *).

Итак, для умножения чисто векторных кватернионов справедлива формула

$$q_1 q_2 = -(q_1, q_2) + [q_1, q_2],$$

где (q_1, q_2) — скалярное, а $[q_1, q_2]$ — векторное произведение векторов q_1 и q_2. Мы видим отсюда, что скалярное и векторное произведения являются как бы «обломками» произведения кватернионов.

Операции скалярного и векторного умножения (наряду со сложением векторов и умножением вектора на число) лежат в основе

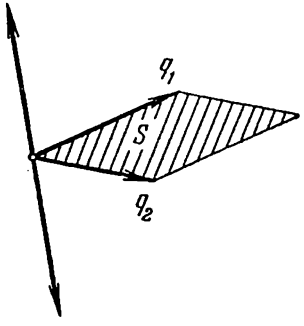


Рис. 4.

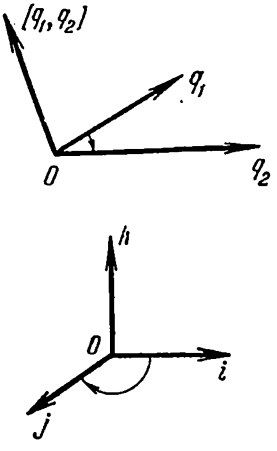


Рис. 5.

целого раздела математики — векторной алгебры, имеющей многочисленные приложения как в самой математике, так и в физике (особенно в механике). Некоторые из этих приложений, вероятно, знакомы читателю (работа есть скалярное произведение вектора силы на вектор перемещения и т. п.). Заметим, что в ясно очерченном виде векторная алгебра появилась значительно позже первых работ по теории кватернионов (труды создателя теории кватернионов английского математика В. Гамильтона относятся к 50-м годам прошлого века, между тем основные положения векторной алгебры были сформулированы в трудах американского математика и физика Д. Гиббса только в 80-х годах прошлого века).

---

*) Вот краткое пояснение этого факта. Представим себе, что концы векторов i и j, перемещаясь в пространстве, приближаются к концам векторов q_1 и q_2 (соответственно). В начальном положении тройка i, j, $[i, j]$ ориентирована подобно i, j, k (ибо $[i, j] = k$). Так как в процессе перемещения ориентация измениться не может, то и конечная тройка q_1, q_2, $[q_1, q_2]$ должна иметь ту же ориентацию, что и i, j, k.

4°. Геометрический смысл умножения произвольного кватерниона на чисто векторный кватернион. Благодаря тому, что умножение кватернионов объединяет в себе два вида умножения векторов (скалярное и векторное), кватернионы являются замечательным средством для решения некоторых задач геометрии и механики. Несколько ниже мы приведем пример весьма трудной задачи, решение которой с помощью кватернионов получается особенно просто и красиво. Однако для этого мы должны поговорить сначала о геометрическом смысле умножения произвольного кватерниона на чисто векторный кватернион.

Пусть

$$q = a + bi + cj + dk$$

— произвольный кватернион, модуль которого равен 1:

$$a^2 + b^2 + c^2 + d^2 = 1.$$

Запишем, что

$$q = a + q',$$

где q' есть вектор $bi + cj + dk$. Так как $|a^2| + |q'|^2 = 1$, то существует такой угол φ, что

$$a = \cos\varphi, \qquad |q'| = \sin\varphi.$$

Очевидно, $q' = |q'|p$, где p — вектор длины 1. Следовательно,

$$q = \cos\varphi + p\sin\varphi.$$

Еще раз подчеркнем, что в таком виде (где p — вектор длины 1) может быть представлен любой кватернион с модулем, равным 1.

Умножим теперь кватернион q на какой-либо векторный кватернион v, причем ограничимся случаем, когда вектор v *перпендикулярен* p. Получим

$$qv = (\cos\varphi + p\sin\varphi)\,v = v\cos\varphi + pv\sin\varphi.$$

Поскольку p и v перпендикулярны, произведение pv будет иметь действительную часть, равную нулю; векторная же часть будет равна $[p, v]$, т. е. вектору длины $|p| \cdot |v| \cdot \sin\frac{\pi}{2} = |v|$, перпендикулярному p и v и ориентированному относительно p и v таким же образом, как вектор k ориентирован относительно i и j. Обозначим этот вектор через $\bar{v}$; можно сказать, что $\bar{v}$ получен из v поворотом вокруг вектора p *) на $\frac{\pi}{2}$. Итак,

$$qv = v\cos\varphi + \bar{v}\sin\varphi.$$

Теперь достаточно взгляда на рис. 6, чтобы понять, что вектор qv получается из v поворотом вокруг оси вектора q на угол φ.

---

*) Слова «поворот вокруг p» звучат несколько двусмысленно, поскольку поворачивать можно в любом из двух направлений. Всюду дальше мы имеем в виду поворот (вокруг p) в том же самом направлении, в каком совершается кратчайший поворот от i к j (вокруг k).

Итак, *если p — какой-либо вектор длины 1, а v — произвольный вектор, перпендикулярный p, то умножение v слева на кватернион*

$$q = \cos\varphi + p\sin\varphi$$

осуществляет поворот вектора v вокруг оси p на угол φ.

До некоторой степени этот факт можно рассматривать как геометрический смысл умножения (слева) на q; разочаровывающим моментом является то, что вектор v выбирается не произвольно, а только перпендикулярно p.

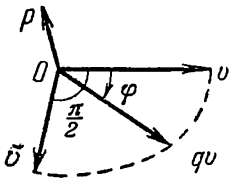


Рис. 6.

5°. Представление произвольного поворота в пространстве с помощью кватернионов. Можно, оказывается, записать в кватернионной форме и поворот вокруг оси p *любого* вектора v, но только для этого придется усложнить действия над v: вместо умножения на q слева потребуется взять более сложное выражение

$$qvq^{-1}.$$

Здесь q^{-1} обозначает кватернион, обратный q, т. е. такой, что $qq^{-1} = 1$. Легко видеть, что

$$q^{-1} = \cos\varphi - p\sin\varphi$$

(действительно, $(\cos\varphi + p\sin\varphi)(\cos\varphi - p\sin\varphi) = \cos^2\varphi - p^2\sin^2\varphi = \cos^2\varphi + \sin^2\varphi = 1$).

Покажем, что *вектор qvq^{-1} получается из v поворотом вокруг оси p на угол 2φ!*

Пусть сначала v перпендикулярен p. Имеем

$$qvq^{-1} = qv(\cos\varphi - p\sin\varphi) = qv\cos\varphi - (qv)p\sin\varphi.$$

Но как мы уже знаем, qv есть снова вектор, перпендикулярный p, поэтому $(qv)p = -p(qv)$. Кватернион $p(qv)$, как мы видели раньше, есть вектор, получаемый из qv поворотом вокруг оси p на угол $\frac{\pi}{2}$ (рис. 7). Обозначим его, как раньше, $\widetilde{qv}$. Итак,

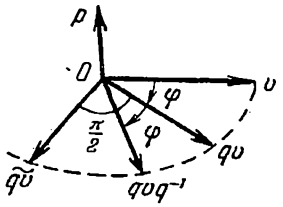


Рис. 7.

$$qvq^{-1} = qv\cos\varphi + \widetilde{qv}\sin\varphi.$$

Выражение, стоящее справа, представляет собой вектор, полученный из qv поворотом вокруг p на угол φ. Если еще учесть, что сам вектор qv получен из v таким же поворотом, то и окажется, что qvq^{-1} получается из v поворотом вокруг p на угол 2φ.

Для того, чтобы рассмотреть общий случай, заметим: если вектор v пропорционален p (т. е. $v = \lambda p$), то, очевидно, $qv = vq$ и

$$qvq^{-1} = vqq^{-1} = v.$$

Пусть теперь v — произвольный вектор. Разложим его на две составляющих: $v = v_1 + v_2$, где v_1 — вектор, перпендикулярный p,

а v_2 пропорционален p. Тогда

$$qvq^{-1} = qv_1q^{-1} + qv_2q^{-1} = qv_1q^{-1} + v_2.$$

Отсюда видно, что составляющая v_1 поворачивается на угол 2φ вокруг p, а составляющая v_2 остается неизменной. В итоге весь вектор v поворачивается вокруг оси p на угол 2φ.

Таким образом, мы доказали, что *при повороте вокруг оси p на угол 2φ произвольный вектор v переходит в qvq^{-1}, где*

$$q = \cos\varphi + p\sin\varphi.$$

Учитывая это, мы скажем, что указанный поворот *соответствует* кватерниону q.

6°. **Задача о «сложении» поворотов.** Еще раньше мы обещали проиллюстрировать применение кватернионов на примере трудной задачи из геометрии. Сделаем это теперь. Задача, о которой будет идти речь, носит название задачи о сложении поворотов (в пространстве).

Пусть производится поворот на угол $2\varphi_1$ вокруг некоторой оси, характеризуемой единичным вектором p_1; следом за ним пусть производится другой поворот — на угол $2\varphi_2$ вокруг оси, характеризуемой единичным вектором p_2. В итоге получим некоторый новый поворот (результат последовательного выполнения двух данных). Спрашивается, как найти ось и угол результирующего поворота?

При первом повороте произвольный вектор v перейдет, как мы знаем, в $v_1 = q_1vq_1^{-1}$, где $q_1 = \cos\varphi_1 + p_1\sin\varphi_1$. При втором повороте v_1 перейдет в

$$v_2 = q_2v_1q_2^{-1} = q_2\left(q_1vq_1^{-1}\right)q_2^{-1} = (q_2q_1)\,v\,(q_2q_1)^{-1}$$

(заметим, что $(q_2q_1)^{-1}$ равно $q_1^{-1}q_2^{-1}$, так как $(q_2q_1)\left(q_1^{-1}q_2^{-1}\right) = 1$). В итоге последовательного выполнения двух поворотов вектор v перейдет в

$$v_2 = (q_2q_1)\,v\,(q_2q_1)^{-1}.$$

Таким образом, *в результате последовательного выполнения двух поворотов, соответствующих кватернионам q_1 и q_2, получается третий поворот, соответствующий кватерниону q_2q_1.*

Вычислить кватернион q_2q_1 не составляет труда — ведь правило умножения кватернионов известно. Найдя q_2q_1, представим этот кватернион в виде

$$q_2q_1 = \cos\psi + p\sin\psi, \tag{5}$$

где p — вектор длины 1. Тогда результирующий поворот есть поворот вокруг оси p на угол 2ψ. Как видим, ответ получился с помощью кватернионов весьма просто!

Рассмотрим пример. Пусть первый поворот совершается вокруг оси x на угол $\frac{\pi}{2}$, а второй — вокруг оси y на тот же угол. Первому повороту отвечает кватернион $q_1 = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2}(1+i)$,

а второму — кватернион $q_2 = \frac{\sqrt{2}}{2}(1 + j)$. В данном случае

$$q_2 q_1 = \frac{1}{2}(1 + j)(1 + i) = \frac{1}{2}(1 + i + j - k).$$

Чтобы представить этот кватернион в виде (5), заметим, что действительная часть его равна $\frac{1}{2} = \cos\frac{\pi}{3}$. Исходя из этого, запишем

$$q_2 q_1 = \cos\frac{\pi}{3} + \left[\frac{1}{\sqrt{3}}(i + j - k)\right]\sin\frac{\pi}{3};$$

таким образом, результирующее вращение происходит вокруг вектора $p = \frac{1}{\sqrt{3}}(i + j - k)$ на угол $\frac{2\pi}{3}$.

§ 5. Гиперкомплексные числа

1°. Определение гиперкомплексной системы чисел. Рассмотренные нами комплексные, двойные, дуальные числа и кватернионы охватываются более общим понятием *гиперкомплексной* (сверхкомплексной) *системы чисел*. Теперь, когда мы знаем наиболее простые примеры таких систем, нам будет легче понять общее определение гиперкомплексной системы чисел.

Зафиксируем натуральное число n и рассмотрим выражения вида

$$a_0 + a_1 i_1 + a_2 i_2 + \ldots + a_n i_n, \qquad (1)$$

где $a_0, a_1, a_2, \ldots, a_n$ — произвольные действительные числа, а $i_1, i_2, \ldots, i_n$ — некоторые символы (которые мы будем иногда называть «мнимыми единицами»). Прежде всего условимся, что равенство двух таких выражений:

$$a_0 + a_1 i_1 + \ldots + a_n i_n = b_0 + b_1 i_1 + \ldots + b_n i_n,$$

означает, по определению, что

$$a_0 = b_0, \quad a_1 = b_1, \ \ldots, \ a_n = b_n.$$

Для сокращенной записи выражений (1) будем пользоваться полужирными латинскими буквами $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, $\boldsymbol{u}$,

v, w, ..., делая исключение только для выражений вида

$$a_0 + 0i_1 + 0i_2 + \ldots + 0i_n,$$

которые иногда будут обозначаться просто a_0.

Над выражениями (1) мы будем производить действия сложения, вычитания и умножения. Сложение и вычитание определяются формулами

$$(a_0 + a_1i_1 + \ldots + a_ni_n) + (b_0 + b_1i_1 + \ldots + b_ni_n) = \\ = (a_0 + b_0) + (a_1 + b_1)i_1 + \ldots + (a_n + b_n)i_n,$$

$$(a_0 + a_1i_1 + \ldots + a_ni_n) - (b_0 + b_1i_1 + \ldots + b_ni_n) = \\ = (a_0 - b_0) + (a_1 - b_1)i_1 + \ldots + (a_n - b_n)i_n,$$

а умножение вводится следующим образом.

Задается «таблица умножения», т. е. указывается, чему равны всевозможные произведения

$$i_\alpha i_\beta,$$

где α и β — любые номера от 1 до n (всего таких произведений имеется, очевидно, $n \times n = n^2$). Каждое произведение $i_\alpha i_\beta$ должно представлять собой снова выражение вида (1), т. е.

$$i_\alpha i_\beta = p_0 + p_1i_1 + p_2i_2 + \ldots + p_ni_n, \qquad (2)$$

где p_0, p_1, ..., p_n — некоторые действительные числа. Любой комбинации номеров α, β отвечает, конечно, свой набор коэффициентов p_0, p_1, ..., p_n; чтобы подчеркнуть зависимость этих коэффициентов от α, β, мы запишем $p_{\alpha\beta, i}$ вместо p_i; тогда (2) заменится, быть может, более громоздким, но зато охватывающим сразу все случаи равенством

$$i_\alpha i_\beta = p_{\alpha\beta, 0} + p_{\alpha\beta, 1}i_1 + p_{\alpha\beta, 2}i_2 + \ldots + p_{\alpha\beta, n}i_n. \qquad (3)$$

Набор чисел $p_{\alpha\beta, \gamma}$ и задает собой таблицу умножения (всего этих чисел должно быть $n^2(n+1)$ — по $n+1$ числу для каждой комбинации α, β).

Например, в случае комплексных чисел таблица умножения состоит из единственного равенства

$$i \cdot i = -1 + 0i.$$

В случае кватернионов таблица содержит девять равенств и может быть записана следующим образом:

	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

Понятно, что каждая клетка заменяет одно из равенств (3) таблицы умножения: например,

$$i \cdot j = k = 0 + 0i + 0j + 1k.$$

После того как задана таблица умножения, мы определяем произведение

$$(a_0 + a_1 i_1 + \ldots + a_n i_n)(b_0 + b_1 i_1 + \ldots + b_n i_n)$$

по обычному правилу умножения суммы на сумму (каждое слагаемое первой суммы умножаем на каждое слагаемое второй и результаты суммируем), причем произведения вида $(a_\alpha i_\alpha) \cdot (b_\beta i_\beta)$ переписываем как $a_\alpha b_\beta (i_\alpha i_\beta)$ и заменяем $i_\alpha i_\beta$ по формуле (3); затем приводим подобные члены. В итоге получается снова некоторое выражение вида (1).

Множество всех выражений вида (1), в котором операции сложения и умножения введены как указано выше, называется *гиперкомплексной системой размерности* $n + 1$, а сами выражения (1) называются *гиперкомплексными числами*. Как следует из приведенного выше описания, гиперкомплексная система данной размерности полностью определяется своей таблицей умножения.

Отметим некоторые свойства операции умножения, справедливые в любой гиперкомплексной системе.

1) Умножение действительного числа a, рассматриваемого как гиперкомплексное число $a + 0i_1 + \ldots + 0i_n$, на произвольное число $b_0 + b_1 i_1 + \ldots + b_n i_n$ сводится

к умножению всех коэффициентов $b_0, b_1, \ldots, b_n$ на a:

$$(a + 0i_1 + \ldots + 0i_n)(b_0 + b_1i_1 + \ldots + b_ni_n) = \\ = ab_0 + ab_1i_1 + \ldots + ab_ni_n$$

и

$$(b_0 + b_1i_1 + \ldots + b_ni_n)(a + 0i_1 + \ldots + 0i_n) = \\ = ab_0 + ab_1i_1 + \ldots + ab_ni_n.$$

В частности,

$$1 \cdot v = v \quad \text{и} \quad v \cdot 1 = v,$$

где v — любое гиперкомплексное число.

2) Если u и v — гиперкомплексные числа, то

$$(au)(bv) = (ab)(uv),$$

где a и b — произвольные действительные числа.

3) Справедливы оба варианта (левый и правый) распределительного закона:

$$u(v + w) = uv + uw,$$
$$(v + w)u = vu + wu.$$

Свойства 1), 2), 3) очевидным образом следуют из самой процедуры умножения. Еще раз подчеркнем, что они справедливы в любой гиперкомплексной системе.

2°. **Коммутативные, ассоциативные системы, системы с делением.** В противоположность указанным выше свойствам другие «хорошие» свойства операции умножения, такие, как

$$uv = vu \qquad \text{(переместительный закон)}$$

и

$$(uv)w = u(vw) \qquad \text{(сочетательный закон)}$$

выполняются далеко не в каждой гиперкомплексной системе. Если для любых двух чисел u и v, принадлежащих данной гиперкомплексной системе, справедливо равенство

$$uv = vu,$$

то такая система называется *коммутативной*.

В этом месте необходимо сделать замечание по поводу дальнейшей терминологии. Дело в том, что в современной математике вместо слов «переместительность» и «сочетательность» приняты имеющие соответ-

ственно тот же смысл термины «коммутативность» и «ассоциативность». Начиная с этого параграфа, мы будем пользоваться только ими.

Рассмотренные ранее системы комплексных чисел, двойных и дуальных являются коммутативными; напротив, система кватернионов не коммутативна.

Нетрудно сообразить, что должно означать условие коммутативности в терминах таблицы умножения (3). Поскольку в случае коммутативной системы должно быть

$$i_\alpha i_\beta = i_\beta i_\alpha \qquad (\alpha, \beta \text{ — любые номера от 1 до } n),$$

то

$$p_{\alpha\beta,0} + p_{\alpha\beta,1} i_1 + \ldots + p_{\alpha\beta,n} i_n = p_{\beta\alpha,0} + p_{\beta\alpha,1} i_1 + \ldots + p_{\beta\alpha,n} i_n$$

и, следовательно,

$$p_{\alpha\beta,0} = p_{\beta\alpha,0}, \quad p_{\alpha\beta,1} = p_{\beta\alpha,1}, \ \ldots, \ p_{\alpha\beta,n} = p_{\beta\alpha,n} \qquad (4)$$

(α, β — любые номера от 1 до n).

Обратно, если выполнены эти равенства, то данная система, очевидно, является коммутативной. Таким образом, наличие соотношений (4) между числами $p_{\alpha\beta,\gamma}$, задающими таблицу умножения, есть необходимое и достаточное условие коммутативности.

В случае, когда для любых трех чисел u, v, w из данной гиперкомплексной системы выполняется равенство

$$(uv)\,w = u\,(vw),$$

система называется *ассоциативной* *).

Условие ассоциативности тоже, разумеется, означает наличие определенных соотношений между числами $p_{\alpha\beta,\gamma}$; каких именно — предоставляем выяснить читателю.

Как мы знаем, системы комплексных, двойных, дуальных чисел, а также кватернионов являются ассоциативными. Простой пример неассоциативной системы дают числа вида $a + bi + cj$ с таблицей умножения

$$i^2 = 0, \quad j^2 = 0, \quad ji = 0, \quad ij = j.$$

В этом случае $(ii)\,j \neq i\,(ij)$.

Согласно определению гиперкомплексных чисел, над ними можно производить действия сложения, вычитания и умножения. Что касается деления, то оно возможно для очень немногих гиперкомплексных систем. Впрочем,

*) Заметим здесь, что, определяя гиперкомплексную систему, мы отступили от исторической традиции. Обычно условие ассоциативности включается в определение гиперкомплексной системы.

здесь следует точно сказать, что подразумевается под возможностью деления.

Говорят, что данная гиперкомплексная система есть *система с делением* (или что в ней возможно деление), если каждое из уравнений

$$vx = u$$

и

$$xv = u$$

имеет решение, и притом единственное, при любых u, v, где $v \neq 0$. Решение первого уравнения называется *левым частным* от деления u на v, решение второго — *правым частным*. Вообще говоря, левое и правое частные не совпадают.

Примерами систем с делением являются комплексные числа и кватернионы. Размерность первой из этих систем равна 2, размерность второй равна 4. Удивительный факт, о котором мы еще будем говорить впоследствии, установлен совсем недавно: гиперкомплексные системы с делением могут иметь только размерности 2, 4 и 8. Отсюда видно, что в общей массе гиперкомплексных систем системы с делением встречаются весьма редко. В частности, гиперкомплексная система, состоящая из чисел вида $a + bi + cj$ с любой таблицей умножения (размерность такой системы равна 3), является системой без деления.

§ 6. Процедура удвоения. Октавы

Мы расскажем здесь еще об одной замечательной системе гиперкомплексных чисел, называемых *октавами*.

Так же, как для комплексных чисел и кватернионов, для октав определены не только сложение, вычитание и умножение, но и деление. Кроме того, рассмотрение октав позволяет сделать еще один шаг в «задаче о сумме квадратов», поставленной в конце § 3, и получить тождество (!) для $n = 8$.

Как показывает само название «октавы» (восьмерные числа), это — выражения, состоящие из восьми членов. Для записи таких выражений необходимо иметь 7 «мнимых единиц» $i_1, i_2, \ldots, i_7$. Итак, октавы — это выражения вида

$$a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3 + a_4 i_4 + a_5 i_5 + a_6 i_6 + a_7 i_7,$$

где a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 — произвольные действительные числа.

Закон умножения октав довольно сложен, поэтому определять его сразу мы не будем. Вместо этого мы опишем одну процедуру, которая позволяет весьма естественным путем строить октавы, исходя из кватернионов. Мы назовем эту процедуру *удвоением**) и определим октавы как «удвоенные» кватернионы. Впрочем, процедура удвоения имеет отношение не только к октавам: мы увидим, что и сами кватернионы получаются удвоением комплексных чисел и, в свою очередь, комплексные числа получаются удвоением действительных чисел.

1°. Другой подход к определению кватернионов. Начнем с некоторого анализа системы кватернионов. Произвольный кватернион

$$q = a + bi + cj + dk$$

можно представить, пользуясь тем, что $ij = k$, в виде

$$q = (a + bi) + (c + di)j$$

или

$$q = z_1 + z_2 j,$$

где $z_1 = a + bi$, $z_2 = c + di$.

Посмотрим, как при таком способе изображения кватернионов запишется их закон умножения.

Пусть наряду с q задан еще один кватернион

$$r = w_1 + w_2 j.$$

Перемножив q и r, получим

$$\begin{aligned} qr &= (z_1 + z_2 j)(w_1 + w_2 j) = \\ &= z_1 w_1 + z_1 (w_2 j) + (z_2 j) w_1 + (z_2 j)(w_2 j) = \\ &= z_1 w_1 + z_1 w_2 j + z_2 j w_1 + z_2 j w_2 j \quad (1) \end{aligned}$$

(мы убрали скобки в произведениях, так как умножение кватернионов обладает свойством ассоциативности). Заметим теперь, что поскольку $ij = -ji$, то $(a + bi)j = j(a - bi)$, т. е.

$$zj = j\bar{z}.$$

---

*) Часто ее называют процедурой Кэли — Диксона, по именам математиков А. Кэли — автора системы октав — и Л. Диксона, впервые рассмотревшего эту процедуру.

Кроме того, легко проверить, что любые два элемента z и w вида $a + bi$ перестановочны:

$$zw = wz.$$

Исходя из этих свойств, можно переписать второе и третье слагаемые в правой части (1) соответственно в виде w_2z_1j и $z_2\overline{w}_1j$, а вместо четвертого слагаемого написать $z_2\overline{w}_2j^2$, или $-\overline{w}_2z_2$. Следовательно,

$$qr = (z_1w_1 - \overline{w}_2z_2) + (w_2z_1 + z_2\overline{w}_1)j. \qquad (2)$$

Обращаясь к представлению кватерниона в виде $q = z_1 + z_2j$, отметим один важный момент. Поскольку $i^2 = -1$, то все кватернионы $a + bi$, в частности, z_1 и z_2, можно трактовать как комплексные числа. Вместе с формулой (2) это приводит нас к такому заключению.

Кватернионы можно определить как выражения вида $z_1 + z_2j$, *где* z_1, z_2 — *произвольные комплексные числа, а* j — *некоторый символ, причем закон умножения таких выражений задается формулой* (2).

Это — очень существенное наблюдение. Оно поможет нам понять процедуру удвоения гиперкомплексных чисел.

2°. Удвоение гиперкомплексной системы. Определение октав. Введем ряд определений. Пусть задана гиперкомплексная система $\mathcal{U}$, состоящая из чисел вида

$$u = a_0 + a_1i_1 + a_2i_2 + \ldots + a_ni_n$$

с некоторым законом умножения.

Условимся называть элемент

$$\overline{u} = a_0 - a_1i_1 - a_2i_2 - \ldots - a_ni_n$$

сопряженным к u.

Удвоением системы $\mathcal{U}$ называется новая гиперкомплексная система $\mathcal{U}^{(2)}$ размерности вдвое большей (чем $\mathcal{U}$), которая строится следующим образом. Ее элементы представляют собой выражения вида

$$u_1 + u_2e, \qquad (3)$$

где u_1, u_2 — произвольные элементы из $\mathcal{U}$, а e — некоторый символ. Сложение элементов из $\mathcal{U}^{(2)}$ производится естественным образом:

$$(u_1 + u_2e) + (v_1 + v_2e) = (u_1 + v_1) + (u_2 + v_2)e, \qquad (4)$$

а умножение определяется по формуле

$$(u_1 + u_2 e)(v_1 + v_2 e) = (u_1 v_1 - \bar{v}_2 u_2) + (v_2 u_1 + u_2 \bar{v}_1) e \quad (5)$$

(черта обозначает сопряжение в $\mathcal{U}$).

Читателю может показаться странным, что, определяя систему $\mathcal{U}^{(2)}$, мы отступили, во-первых, от обычного способа записи гиперкомплексных чисел, и, во-вторых, от задания умножения с помощью таблицы. Числа из $\mathcal{U}^{(2)}$ должны были бы иметь вид

$$a_0 + a_1 i_1 + \ldots + a_n i_n + a_{n+1} i_{n+1} + \ldots + a_{2n+1} i_{2n+1}, \quad (6)$$

однако мы предпочитаем более короткую запись (3). Дело в том, что каждому выражению (6) можно сопоставить два элемента исходной гиперкомплексной системы:

$$u_1 = a_0 + a_1 i_1 + \ldots + a_n i_n,$$
$$u_2 = a_{n+1} + a_{n+2} i_1 + \ldots + a_{2n+1} i_n,$$

а значит, и выражение (3) (оно является как бы «кодом» гиперкомплексного числа (6)); и обратно, разумеется, если задано выражение вида (6), то по нему можно составить (3). Краткая запись (3) по сравнению с (6) имеет существенное преимущество: вместо того, чтобы задавать умножение в $\mathcal{U}^{(2)}$ с помощью таблицы, мы можем записать его в обозримой форме (5). Конечно, из формулы (5) можно извлечь таблицу умножения «мнимых единиц» $i_1, i_2, \ldots, i_{2n+1}$. В общем виде заниматься этой таблицей мы не будем, но для наиболее интересующего нас случая октав приведем ее дальше полностью.

Итак, мы определили процедуру удвоения. Примером может служить переход от комплексных чисел к кватернионам: то, что было сделано в начале этого параграфа, фактически означает, что система кватернионов есть удвоение системы комплексных чисел. Легко также проверить (читателю рекомендуется сделать это самостоятельно), что комплексные числа получаются удвоением действительных.

Главной целью этого параграфа, как уже говорилось, является построение системы октав. Определение октав может быть сформулировано теперь в нескольких словах: *система октав есть удвоение системы кватернионов.* Все свойства системы октав получаются, естественно, из

данного определения; начиная со следующего пункта, мы переходим к подробному изучению этих свойств.

3°. Таблица умножения в системе октав. Итак, согласно определению, октавы — это выражения вида

$$q_1 + q_2 e,$$

где q_1, q_2 — произвольные кватернионы, причем закон умножения имеет следующий вид:

$$(q_1 + q_2 e)(r_1 + r_2 e) = (q_1 r_1 - \bar{r}_2 q_2) + (r_2 q_1 + q_2 \bar{r}_1) e. \quad (7)$$

Прежде всего посмотрим, как увязывается такое определение октав с представлением октав в форме

$$a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3 + a_4 i_4 + a_5 i_5 + a_6 i_6 + a_7 i_7, \quad (8)$$

точнее, составим таблицу умножения для мнимых единиц $i_1, \ldots, i_7$.

Кватернионы q_1 и q_2, отвечающие записи (8), суть

$$q_1 = a_0 + a_1 i + a_2 j + a_3 k, \quad q_2 = a_4 + a_5 i + a_6 j + a_7 k.$$

Договоримся для большего единообразия вместо (8) писать

$$a + bi + cj + dk + AE + BI + CJ + DK,$$

где a, b, c, d, A, B, C, D — это прежние $a_0, a_1, \ldots, a_7$, а i, j, k, E, I, J, K — новые обозначения для «мнимых единиц» $i_1, i_2, \ldots, i_7$.

В таких обозначениях кватернионы q_1 и q_2 будут

$$q_1 = a + bi + cj + dk, \quad q_2 = A + Bi + Cj + Dk.$$

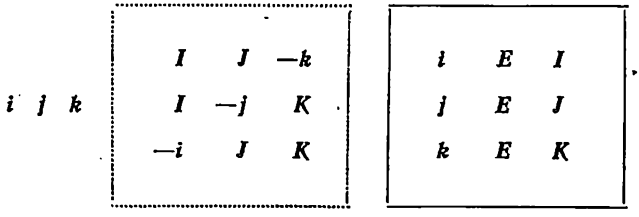
Исходя из (7), можно, как уже отмечалось, составить таблицу умножения для единиц i, j, k, E, I, J, K. Например, полагая в формуле (7) $q_2 = r_2 = 0$, получим

$$(q_1 + 0e)(r_1 + 0e) = q_1 r_1 + 0e;$$

таким образом, октавы q_1 и r_1 перемножаются как кватернионы. Отсюда следует, что для единиц i, j, k таблица умножения в точности такая же, как в случае кватернионов:

$$i^2 = -1, \quad j^2 = -1, \quad k^2 = -1,$$
$$ij = k, \quad ji = -k,$$
$$jk = i, \quad kj = -i,$$
$$ki = j, \quad ik = -j.$$

Написанные равенства дают выражения только для 9 произведений из общего числа 49 (в нашем случае имеется 7 единиц и, следовательно, $7 \cdot 7 = 49$ попарных произведений). Выписывать остальные 40 произведений нет необходимости, так как существует довольно простой способ запомнить всю таблицу. Он состоит в указании следующих семи троек:



Запомнить эти тройки нетрудно: каждая тройка в пунктирной рамке получается из тройки символов i, j, k, если перед одним из них поставить знак минус, а два других заменить на соответствующие заглавные символы; каждая из троек в сплошной рамке содержит E и два одноименных символа.

Чтобы объяснить таблицу умножения, обозначим α, β, γ любую из указанных семи троек (порядок символов в тройке существен). Тогда

$$\alpha\beta = \gamma, \quad \beta\alpha = -\gamma,$$
$$\beta\gamma = \alpha, \quad \gamma\beta = -\alpha,$$
$$\gamma\alpha = \beta, \quad \alpha\gamma = -\beta,$$

и

$$\alpha^2 = -1, \quad \beta^2 = -1, \quad \gamma^2 = -1,$$

т. е. α, β, γ перемножаются в точности так же, как кватернионы i, j, k.

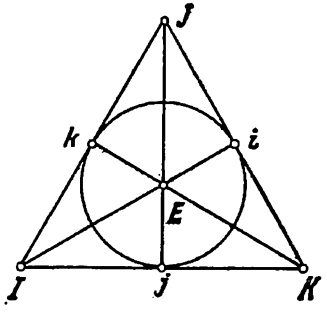


Рис. 8.

Хорошей иллюстрацией к этому правилу служит рис. 8. На нем изображен треугольник с вершинами I, J, K и серединами сторон i, j, k; в точке пересечения медиан поставлена буква E. На каждой прямой лежат три «мнимые» единицы. Кроме того, три единицы i, j, k также считаются принадлежащими одной «прямой» (символически обозначенной на рисунке окружностью). Итак, на рисунке имеется 7 «прямых» и на каждой из них расположены три единицы. Для того, чтобы найти произведение любых двух единиц, нужно рассмотреть «прямую», определяемую этими единицами, и взять третью единицу этой «прямой» со знаком + или —.

Любопытно, что единицы i, j, k, E, I, J, K могут быть расставлены на этом чертеже многими способами. Достаточно взять i, j, k лежащими на одной «прямой» (любой из семи), какую-нибудь из оставшихся точек обозначить E и затем проставить I, J, K на прямых iE, jE, kE; в результате мы придем снова к правильной картине.

4°. Сопряжение в системе октав. Модуль октавы. Пусть

$$u = a + bi + cj + dk + AE + BI + CJ + DK \qquad (9)$$

— произвольная октава. Октаву

$$\bar{u} = a - bi - cj - dk - AE - BI - CJ - DK$$

будем называть *сопряженной к* u.

Если вместо (9) воспользоваться более короткой записью

$$u = q_1 + q_2 e,$$

где

$$q_1 = a + bi + cj + dk, \quad q_2 = A + Bi + Cj + Dk,$$

то для сопряженной октавы получится выражение

$$\bar{u} = \bar{q}_1 - q_2 e.$$

Вычислим теперь, чему равно произведение произвольной октавы u на сопряженную октаву $\bar{u}$. Мы увидим, что это произведение, как и в случае комплексных чисел или кватернионов, равно действительному числу (т. е. октаве вида $a + 0i + 0j + \ldots + 0K$).

Имеем

$$u\bar{u} = (q_1 + q_2 e)(\bar{q}_1 - q_2 e) = (q_1\bar{q}_1 + \bar{q}_2 q_2) + (-q_2 q_1 + q_2 q_1) e.$$

Учитывая, что для кватернионов $q\bar{q} = \bar{q}q = |q|^2$, находим отсюда

$$u\bar{u} = q_1\bar{q}_1 + q_2\bar{q}_2 = |q_1|^2 + |q_2|^2. \qquad (10)$$

Квадратный корень из выражения $|q_1|^2 + |q_2|^2$ называется *модулем* или *нормой* октавы u и обозначается $|u|$. Заметим, что для октавы u, заданной в форме (9), квадрат ее модуля равен

$$a^2 + b^2 + c^2 + d^2 + A^2 + B^2 + C^2 + D^2. \qquad (11)$$

Таким образом, по определению модуля имеем

$$u\bar{u} = |u|^2; \qquad (12)$$

к этому равенству можно добавить другое:

$$\bar{u}u = |u|^2,$$

вытекающее из того факта, что квадрат модуля октавы u совпадает с квадратом модуля сопряженной октавы $\bar{u}$ (и то и другое равно (11)).

5°. **Модуль произведения октав.** Система октав имеет много общего с системами комплексных чисел и кватернионов. Одним из проявлений этой общности является то важнейшее свойство, что модуль произведения любых двух октав равен произведению модулей этих октав:

$$|uv| = |u||v| \tag{13}$$

или, что эквивалентно,

$$|uv|^2 = |u|^2|v|^2. \tag{14}$$

Доказательство равенства (14) можно провести непосредственным вычислением. Подсчитаем по отдельности $|uv|^2$ и $|u|^2|v|^2$. Так как

$$uv = (q_1 + q_2 e)(r_1 + r_2 e) = (q_1 r_1 - \bar{r}_2 q_2) + (r_2 q_1 + q_2 \bar{r}_1) e,$$

то, применив формулу (10), получим

$$|uv|^2 = (q_1 r_1 - \bar{r}_2 q_2)\overline{(q_1 r_1 - \bar{r}_2 q_2)} + (r_2 q_1 + q_2 \bar{r}_1)\overline{(r_2 q_1 + q_2 \bar{r}_1)}$$

или, учитывая свойства сопряжения для кватернионов,

$$|uv|^2 = (q_1 r_1 - \bar{r}_2 q_2)(\bar{r}_1 \bar{q}_1 - \bar{q}_2 r_2) + (r_2 q_1 + q_2 \bar{r}_1)(\bar{q}_1 \bar{r}_2 + r_1 \bar{q}_2).$$

С другой стороны,

$$|u|^2 |v|^2 = (q_1 \bar{q}_1 + q_2 \bar{q}_2)(r_1 \bar{r}_1 + r_2 \bar{r}_2).$$

Сравнивая оба выражения, находим, что они отличаются на сумму четырех слагаемых

$$S = r_2 q_1 r_1 \bar{q}_2 + q_2 \bar{r}_1 \bar{q}_1 \bar{r}_2 - q_1 r_1 \bar{q}_2 \bar{r}_2 - \bar{r}_2 q_2 \bar{r}_1 \bar{q}_1.$$

Поэтому остается показать, что $S = 0$ для любых четырех кватернионов q_1, q_2, r_1, r_2.

Начнем с очевидного замечания: $S = 0$, если r_2 — действительное число. С другой стороны, если r_2 есть чисто мнимый кватернион (и, следовательно, $\bar{r}_2 = -r_2$), то

$$S = r_2 (q_1 r_1 \bar{q}_2 + q_2 \bar{r}_1 \bar{q}_1) - (q_1 r_1 \bar{q}_2 + q_2 \bar{r}_1 \bar{q}_1) r_2.$$

Выражение в скобках представляет собой сумму двух сопряженных кватернионов и поэтому равно

действительному числу; обозначим его c. Тогда

$$S = r_2 c - c r_2 = 0.$$

Теперь следует учесть очевидное свойство выражения S: если оно равно 0 при $r_2 = a$ и $r_2 = b$, то оно равно 0 при $r_2 = a + b$. Так как любой кватернион r_2 представляется в виде суммы действительного числа и чисто мнимого кватерниона, причем в обоих случаях $S = 0$, то тем самым S равно нулю тождественно.

6°. Тождество для восьми квадратов. Установленное в предыдущем пункте равенство

$$|uv|^2 = |u|^2 |v|^2 \tag{15}$$

означает новый вклад в решение «задачи о сумме квадратов», поставленной в конце § 3, так как в подробной записи оно представляет собой (если читать его справа налево) тождество: «*произведение суммы восьми квадратов на сумму восьми квадратов есть снова сумма восьми квадратов*». Действительно, пусть

$$u = a + bi + cj + dk + AE + BI + CJ + DK,$$
$$v = a' + b'i + c'j + d'k + A'E + B'I + C'J + D'K,$$

а

$$uv = \Phi_0 + \Phi_1 i + \Phi_2 j + \Phi_3 k + \Phi_4 E + \Phi_5 I + \Phi_6 J + \Phi_7 K,$$

тогда равенство (15) принимает вид

$$(a^2 + \ldots + D^2)(a'^2 + \ldots + D'^2) = \Phi_0^2 + \Phi_1^2 + \ldots + \Phi_7^2.$$

Разумеется, вместо Φ_0, Φ_1, ..., Φ_7 сюда следует подставить их выражения через a, ..., D, a', ..., D', исходя из закона умножения октав. Проделав эту громоздкую работу, придем к такому тождеству:

$$\begin{aligned}
&(a^2 + b^2 + c^2 + d^2 + A^2 + B^2 + C^2 + D^2) \times \\
&\quad \times (a'^2 + b'^2 + c'^2 + d'^2 + A'^2 + B'^2 + C'^2 + D'^2) = \\
&= (aa' - bb' - cc' - dd' - AA' - BB' - CC' - DD')^2 + \\
&+ (ab' + ba' + cd' - dc' - A'B + B'A + C'D - D'C)^2 + \\
&+ (ac' + ca' - bd' + db' - A'C + C'A - B'D + D'B)^2 + \\
&+ (ad' + da' + bc' - cb' - A'D + D'A + B'C - C'B)^2 + \\
&+ (A'a - B'b - C'c - D'd + Aa' + Bb' + Cc' + Dd')^2 + \\
&+ (A'b + B'a + C'd - D'c - Ab' + Ba' - Cd' + Dc')^2 + \\
&+ (A'c + C'a - B'd + D'b - Ac' + Ca' + Bd' - Db')^2 + \\
&+ (A'd + D'a + B'c - C'b - Ad' + Da' - Bc' + Cb')^2.
\end{aligned}$$

Интересно отметить, что именно поиски тождества для 8 квадратов привели автора системы октав английского-математика А. Кэли к их открытию!

7°. Неассоциативность октав. Свойство альтернативности. Выше говорилось, что многие свойства октав сходны со свойствами кватернионов и комплексных чисел. Сейчас мы обратим внимание на одно существенное различие между этими системами: в то время как умножение комплексных чисел и кватернионов обладает ассоциативным (сочетательным) свойством, *для умножения октав ассоциативный закон не выполняется.* Например,

$$(ij)E \neq i(jE),$$

так как $(ij)E = kE = K$, а $i(jE) = iJ = -K$.

Отсутствие ассоциативного закона для октав вовсе не означает, что для *любых* трех октав u, v, w будет $(uv)w \neq u(vw)$. Более того, можно доказать, что *справедливы следующие две формулы*:

$$(uv)v = u(vv) \tag{16}$$

и

$$v(vu) = (vv)u, \tag{17}$$

в которых u и v обозначают любые две октавы.

Формулы (16) и (17) можно рассматривать как некий ослабленный вариант ассоциативности. Существует специальное название для систем, в которых справедливы эти формулы; такие системы называются *альтернативными.*

Обращаясь к доказательству формул (16) и (17), заметим, что вместо них можно доказывать

$$(uv)\bar{v} = u(v\bar{v}) \tag{16'}$$

и

$$\bar{v}(vu) = (\bar{v}v)u, \tag{17'}$$

так как, заменяя в этих равенствах $\bar{v}$ на $-v + 2a$ (где a — действительная часть октавы v), легко получим (16) и (17).

Докажем формулу (16'); формула (17') получается аналогично.

Пусть $u = q_1 + q_2 e$, $v = r_1 + r_2 e$. Имеем

$$\begin{aligned}(uv)\bar{v} &= ((q_1 + q_2 e)(r_1 + r_2 e))(\bar{r}_1 - r_2 e) = \\ &= ((q_1 r_1 - \bar{r}_2 q_2) + (r_2 q_1 + q_2 \bar{r}_1) e)(\bar{r}_1 - r_2 e) = \\ &= ((q_1 r_1 - \bar{r}_2 q_2)\bar{r}_1 + \bar{r}_2 (r_2 q_1 + q_2 \bar{r}_1)) + \\ &+ ((-r_2)(q_1 r_1 - \bar{r}_2 q_2) + (r_2 q_1 + q_2 \bar{r}_1) r_1) e = \\ &= (|r_1|^2 + |r_2|^2) q_1 + (|r_1|^2 + |r_2|^2) q_2 e = \\ &= (|r_1|^2 + |r_2|^2)(q_1 + q_2 e) = |v|^2 u.\end{aligned}$$

С другой стороны, $|v\bar{v}| = |v|^2$, поэтому

$$u(v\bar{v}) = |v|^2 u.$$

Отсюда следует (16′).

8°. **Октавы — система с делением.** Еще одно важное свойство системы октав, сближающее их с комплексными числами и кватернионами, есть *возможность деления*. Пусть u и v — произвольные октавы, причем $v \neq 0$. Напомним, что левое частное от деления u на v есть решение уравнения

$$vx = u, \tag{18}$$

а правое частное — решение уравнения

$$xv = u. \tag{19}$$

Решим сначала уравнение (18). Поступая точно так же, как в случае кватернионов, умножим обе части (18) слева на $\bar{v}$. Получим

$$\bar{v}(vx) = \bar{v}u$$

или, учитывая (17′),

$$|v|^2 x = \bar{v}u.$$

Отсюда

$$x = \frac{1}{|v|^2}\bar{v}u.$$

Непосредственная проверка (с использованием опять-таки формулы (17′)) показывает, что найденное значение x удовлетворяет уравнению (18). Итак, левое частное от деления u на v равно

$$x_л = \frac{1}{|v|^2}\bar{v}u.$$

Аналогично доказывается, что правое частное равно

$$x_{\text{п}} = \frac{1}{|v|^2}\,\bar{u}v;$$

при этом нужно воспользоваться формулой (16′).

Мы видим, таким образом, что октавы образуют *систему с делением.*

§ 7. Алгебры

1°. Наводящие соображения. Вернемся еще раз к общему понятию гиперкомплексной системы. Согласно определению, данному в § 5, гиперкомплексная система размерности $n+1$ есть множество выражений вида

$$a_0 + a_1 i_1 + a_2 i_2 + \ \dots\ + a_n i_n$$

(гиперкомплексных чисел) с естественным правилом сложения и некоторым правилом умножения. Последнее заключается в том, что задается таблица вида

$$i_\alpha i_\beta = p_{\alpha\beta,0} + p_{\alpha\beta,1} i_1 + \ \dots\ + p_{\alpha\beta,n} i_n \qquad (1)$$

(таблица умножения «мнимых единиц» $i_1, i_2, \dots, i_n$), после чего произведение двух гиперкомплексных чисел определяется по правилу умножения суммы на сумму, с последующей записью слагаемых $(a_\alpha i_\alpha)(b_\beta i_\beta)$ в виде $a_\alpha b_\beta (i_\alpha i_\beta)$ и заменой произведений $i_\alpha i_\beta$ по формулам (1).

Рассмотрим такой случай, когда все числа $p_{\alpha\beta,0}$ («свободные члены» в формулах (1)) равны нулю. Тогда произведение любых двух мнимых единиц i_α, i_β есть снова комбинация мнимых единиц.

Обозначим через $\mathscr{A}$ множество всех гиперкомплексных чисел вида

$$a = a_1 i_1 + a_2 i_2 + \ \dots\ + a_n i_n \qquad (2)$$

(без свободных членов). Совершенно очевидно, что сумма двух таких чисел есть снова число вида (2). Из того, что сказано выше относительно произведений $i_\alpha i_\beta$, следует, что и умножение двух чисел вида (2) дает снова число вида (2). Таким образом, множество $\mathscr{A}$ обладает тем свойством, что обе операции — сложение и умножение — не выводят за пределы этого множества. Наличие такого свойства позволяет рассматривать $\mathscr{A}$

как *самостоятельную систему* с двумя операциями — сложением и умножением. Однако она не является, вообще говоря, гиперкомплексной системой в том смысле, какой мы придаем этому слову (о тех случаях, когда систему $\mathscr{A}$ все же можно рассматривать как гиперкомплексную, мы скажем чуть позже).

Главное отличие системы $\mathscr{A}$ от гиперкомплексной сводится к следующему. Каждая гиперкомплексная система обязана содержать некоторый особенный элемент e такой, что

$$e \cdot a = a \cdot e = a$$

для любого элемента a из данной системы (этим элементом e является $1 + 0i_1 + \ldots + 0i_n$); между тем в системе $\mathscr{A}$ элемент с таким свойством, вообще говоря, не существует. Имеется и еще одно отличие, тесно связанное с первым: в гиперкомплексной системе можно говорить о произведении действительного числа k на любой элемент a данной системы (по определению, это есть произведение элементов $k = k + 0i_1 + \ldots + 0i_n$ и a); в системе $\mathscr{A}$, напротив, произведение ka не имеет смысла. Однако это последнее отличие легко устранить: для этого достаточно *ввести* операцию умножения действительного числа на элементы из $\mathscr{A}$ по формуле

$$k(a_1i_1 + a_2i_2 + \ldots + a_ni_n) = ka_1i_1 + ka_2i_2 + \ldots + ka_ni_n.$$

Снабженное такой операцией, множество $\mathscr{A}$ (с уже имеющимися в нем сложением и умножением) превращается в объект, носящий специальное название *алгебра размерности n* или просто *алгебра* *).

2°. Определение алгебры. Дадим теперь точное определение алгебры.

Алгеброй размерности n называется множество выражений вида

$$a_1i_1 + a_2i_2 + \ldots + a_ni_n \qquad (2)$$

(где $a_1, a_2, \ldots, a_n$ — произвольные действительные числа, а $i_1, i_2, \ldots, i_n$ — некоторые символы), снабженное следующими операциями:

*) Таким образом, слово «алгебра» имеет два смысла: алгебра как раздел математики и алгебра как математический объект с определенными свойствами.

1) операцией умножения на действительные числа, выполняемой по формуле:

$$k(a_1 i_1 + a_2 i_2 + \ldots + a_n i_n) = ka_1 i_1 + ka_2 i_2 + \ldots + ka_n i_n; \quad (3)$$

2) операцией сложения:

$$(a_1 i_1 + a_2 i_2 + \ldots + a_n i_n) + (b_1 i_1 + b_2 i_2 + \ldots + b_n i_n) = \\ = (a_1 + b_1) i_1 + (a_2 + b_2) i_2 + \ldots + (a_n + b_n) i_n; \quad (4)$$

3) операцией умножения, задаваемой таблицей вида

$$i_\alpha i_\beta = p_{\alpha\beta,1} i_1 + p_{\alpha\beta,2} i_2 + \ldots + p_{\alpha\beta,n} i_n, \quad (5)$$

где α, β — любые номера от 1 до n (таблица используется для нахождения произведений

$$(a_1 i_1 + a_2 i_2 + \ldots + a_n i_n)(b_1 i_1 + b_2 i_2 + \ldots + b_n i_n)$$

в точности так же, как в случае гиперкомплексной системы).

Из данного выше определения алгебры видно, что алгебра размерности n полностью определяется своей «таблицей умножения» (5), т. е. некоторым набором n^3 чисел $p_{\alpha\beta,\gamma}$. В принципе эти числа не подчинены никаким условиям; любой набор их задает некоторую алгебру.

3°. **Гиперкомплексная система — частный случай алгебры.** Хотя для большей ясности изложения мы «извлекли» понятие алгебры из понятия гиперкомплексной системы, следует отчетливо уяснить, что понятие алгебры — более широкое; иначе говоря, что *любая гиперкомплексная система может рассматриваться как алгебра той же размерности.* Разъясним это подробнее.

Пусть дана алгебра $\mathcal{A}$, состоящая из элементов

$$a_1 i_1 + a_2 i_2 + \ldots + a_n i_n$$

с таблицей умножения

$$i_\alpha i_\beta = p_{\alpha\beta,1} i_1 + p_{\alpha\beta,2} i_2 + \ldots + p_{\alpha\beta,n} i_n$$

(α, β — любые номера от 1 до n),

причем единица i_1 обладает особым свойством:

$$i_1 i_\alpha = i_\alpha \quad \text{и} \quad i_\alpha i_1 = i_\alpha \quad \text{для всех } \alpha \text{ от 1 до } n. \quad (6)$$

Рассмотрим наряду с ней гиперкомплексную систему, состоящую из элементов

$$a_1 + a_2 i_2 + \ldots + a_n i_n$$

с таблицей умножения

$$i_\alpha i_\beta = p_{\alpha\beta,1} + p_{\alpha\beta,2} i_2 + \ldots + p_{\alpha\beta,n} i_n$$

(α, β — любые номера от 2 до n);

эту гиперкомплексную систему будем рассматривать как *соответствующую* алгебре $\mathscr{A}$.

Пользуясь таблицей умножения, можно найти произведение любых двух элементов данной алгебры:

$$(a_1 i_1 + a_2 i_2 + \ldots + a_n i_n)(b_1 i_1 + b_2 i_2 + \ldots + b_n i_n) = \\ = c_1 i_1 + c_2 i_2 + \ldots + c_n i_n.$$

Если теперь в написанном равенстве «убрать» i_1, то получится соотношение

$$(a_1 + a_2 i_2 + \ldots + a_n i_n)(b_1 + b_2 i_2 + \ldots + b_n i_n) = \\ = c_1 + c_2 i_2 + \ldots + c_n i_n,$$

которое ввиду (6) будет выражать закон умножения в соответствующей гиперкомплексной системе.

Таким образом, любая алгебра с условием (6) «вычеркиванием» символа i_1 из записи всех элементов превращается в гиперкомплексную систему той же размерности.

Более того, поскольку числа $p_{\alpha\beta,\gamma}$ для $\alpha > 1$, $\beta > 1$ в предыдущем рассуждении произвольны, то указанным путем может быть получена *любая* гиперкомплексная система.

Для иллюстрации рассмотрим пример. Пусть задана двумерная алгебра $\mathscr{A}$ с такой таблицей умножения:

$$i_1 i_1 = i_1, \quad i_1 i_2 = i_2, \quad i_2 i_1 = i_2, \quad i_2 i_2 = -i_1.$$

Равенства (6) здесь, очевидно, выполняются. Закон умножения в $\mathscr{A}$ выглядит следующим образом:

$$(a_1 i_1 + a_2 i_2)(b_1 i_1 + b_2 i_2) = (a_1 b_1 - a_2 b_2) i_1 + (a_1 b_2 + a_2 b_1) i_2.$$

Если «вычеркнуть» i_1, то таблица умножения превратится в

$$i_2 i_2 = -1,$$

а закон умножения примет вид

$$(a_1 + a_2 i_2)(b_1 + b_2 i_2) = (a_1 b_1 - a_2 b_2) + (a_1 b_2 + a_2 b_1) i_2,$$

откуда сразу же становится ясным, что рассматриваемая алгебра совпадает, по существу, с системой комплексных чисел.

4°. Коммутативные, ассоциативные алгебры, алгебры с делением. В § 5 мы ввели ряд терминов для обозначения некоторых свойств гиперкомплексных систем. Эта терминология без всяких изменений переносится на алгебры. А именно, если для любых двух элементов a и b алгебры $\mathcal{A}$ справедливо равенство

$$ab = ba,$$

то алгебра называется *коммутативной*; если для любых трех элементов a, b и c справедливо равенство

$$(ab)c = a(bc),$$

то алгебра называется *ассоциативной* *). Далее, если каждое из уравнений

$$ax = b \tag{7}$$

и

$$ya = b, \tag{8}$$

где a и b — произвольные элементы алгебры $\mathcal{A}$, причем $a \neq 0$, имеет единственное решение, то говорят, что $\mathcal{A}$ есть *алгебра с делением*; элемент x, определяемый из уравнения (7), называется в этом случае *левым частным*, а элемент y, определяемый из (8), — *правым частным* от деления b на a.

Нетрудно видеть, что в алгебрах с делением справедливо такое свойство: *если произведение ab равно нулю, то хотя бы один из сомножителей a или b равен нулю.*

Действительно, если $a \neq 0$, то $b = 0$, ибо единственным решением уравнения $ax = 0$ является $x = 0$.

Позднее мы докажем (см. § 9), что справедливо и обратное предложение:

если алгебра $\mathcal{A}$ обладает тем свойством, что из равенства нулю произведения ab следует равенство нулю хотя бы одного из сомножителей a или b, то $\mathcal{A}$ есть алгебра с делением.

---

*) На первоначальном этапе развития теории алгебр условие ассоциативности представлялось настолько естественным, что его включали в определение алгебры; под термином «алгебра» понималась «ассоциативная алгебра».

Если в алгебре $\mathcal{A}$ существует такой элемент e, что

$$ae = a \quad \text{и} \quad ea = a$$

для любого $a \in \mathcal{A}$, то этот элемент называется *единицей алгебры* $\mathcal{A}$; в этом случае также говорят, что $\mathcal{A}$ есть *алгебра с единицей*. Любая гиперкомплексная система является, как уже отмечалось, алгеброй с единицей.

Простейшим примером алгебры с единицей является одномерная алгебра с таблицей умножения

$$i_1 i_1 = i_1.$$

Закон умножения в этой алгебре имеет вид

$$(a_i i_1)(b_1 i_1) = a_1 b_1 i_1,$$

т. е. сводится к умножению действительных чисел. В соответствии с этим указанную алгебру будем называть *алгеброй действительных чисел*.

5°. **Примеры.** Рассмотрим некоторые примеры алгебр, не являющихся гиперкомплексными системами.

Пример 1. *Нулевая алгебра произвольной размерности n.* Таблица умножения в этой алгебре имеет предельно простой вид:

$$i_\alpha i_\beta = 0 \qquad \text{(для всех номеров } \alpha, \beta \text{ от 1 до } n).$$

Отсюда сразу следует, что произведение любых двух элементов также равно нулю.

Пример 2. Рассмотрим двумерную алгебру с таблицей умножения

$$i_1 i_1 = i_1,$$
$$i_1 i_2 = i_2,$$
$$i_2 i_1 = -i_2,$$
$$i_2 i_2 = i_1.$$

Тогда закон умножения будет

$$(a_1 i_1 + a_2 i_2)(b_1 i_1 + b_2 i_2) = (a_1 b_1 + a_2 b_2) i_1 + (a_1 b_2 - a_2 b_1) i_2.$$

Хотя в этой алгебре умножение напоминает умножение комплексных чисел, однако она не совпадает с алгеброй комплексных чисел. Предлагаем читателю проверить самостоятельно, что в этой алгебре нет единицы (тем самым она не может являться гиперкомплексной системой). Более сложным упражнением является про-

верка того интересного факта, что рассматриваемая алгебра есть алгебра с делением.

Пример 3. *Алгебра трехмерных векторов с операцией векторного произведения.* Эта алгебра состоит из элементов вида

$$bi + cj + dk,$$

перемножаемых в соответствии с таблицей

$$\begin{aligned} i^2 = 0, \quad & j^2 = 0, \quad k^2 = 0, \\ ij = k, \quad & ji = -k, \\ jk = i, \quad & kj = -i, \\ ki = j, \quad & ik = -j. \end{aligned}$$

Таким образом,

$$\begin{aligned} (bi + cj + dk)(b'i + c'j + d'k) = \\ = (cd' - dc')i + (db' - bd')j + (bc' - cb')k. \end{aligned} \quad (9)$$

Если ввести в обычном пространстве прямоугольную систему координат и под i, j, k понимать векторы длины 1, имеющие направления координатных осей (рис. 9), то выражение

$$q = bi + cj + dk$$

будет представлять собой (при обычном геометрическом понимании суммы векторов и произведения вектора на число) некоторый вектор в пространстве. Операция (9) носит название векторного произведения (ее геометрический смысл см. в § 4); она играет важную роль в геометрии и физике.

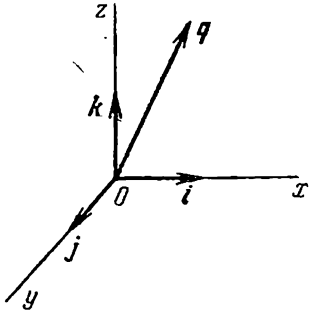


Рис. 9.

6°. Важный пример: алгебра квадратных матриц n-го порядка. Размерность этой алгебры равна n^2. Соответствующие мнимые единицы можно было бы обозначить $i_1, i_2, \ldots, i_{n^2}$, но более удобным является другой принцип нумерации: вместо номера α, пробегающего значения от 1 до n^2, удобнее пользоваться «номером», состоящим из двух чисел α, β, каждое из которых пробегает значения от 1 до n (очевидно, число различных пар α, β будет в точности n^2). Таким образом, для мнимых единиц мы вводим обозначение $i_{\alpha\beta}$. Порядок следования мнимых единиц можно установить как угодно;

для определенности будем располагать их в такой последовательности:

$$i_{11},\ i_{12},\ \ldots,\ i_{1n} \mid i_{21},\ i_{22},\ \ldots,\ i_{2n} \mid i_{31},\ i_{32},\ \ldots$$
$$\ldots,\ i_{3n} \mid \ldots \mid i_{n1},\ i_{n2},\ \ldots,\ i_{nn}.$$

Итак, элементами нашей алгебры являются выражения следующего вида:

$$\begin{aligned} A = {} & a_{11}i_{11} + a_{12}i_{12} + \ldots + a_{1n}i_{1n} + \\ & + a_{21}i_{21} + a_{22}i_{22} + \ldots + a_{2n}i_{2n} + \\ & \ldots\ldots\ldots\ldots\ldots \\ & + a_{n1}i_{n1} + a_{n2}i_{n2} + \ldots + a_{nn}i_{nn}. \end{aligned} \tag{10}$$

В такой записи становится особенно ясным тот факт, что произвольный элемент A нашей алгебры определяется таблицей

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix},$$

состоящей из n^2 чисел. Такие таблицы носят название *матриц*, точнее, *квадратных матриц порядка n* (порядком называется число строк или столбцов в квадратной таблице). В дальнейшем вместо (10) мы позволим себе писать кратко:

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

и считать, что *элементы нашей алгебры суть матрицы.*

Определим теперь таблицу умножения единиц $i_{\alpha\beta}$; в ней и заключено все своеобразие алгебры матриц.

Положим

$$i_{\alpha 1}i_{1\beta} = i_{\alpha\beta},\ i_{\alpha 2}i_{2\beta} = i_{\alpha\beta},\ \ldots,\ i_{\alpha n}i_{n\beta} = i_{\alpha\beta} \tag{11}$$

или короче,

$$i_{\alpha\lambda}i_{\lambda\beta} = i_{\alpha\beta} \qquad (\alpha,\ \beta,\ \lambda — \text{любые номера от 1 до } n);$$

все остальные произведения мнимых единиц по определению равны нулю. Этим таблица умножения задана полностью.

Впрочем, можно записать всю таблицу умножения в более сжатой форме:

$$i_{\alpha\lambda} i_{\mu\beta} = \delta_{\lambda\mu} i_{\alpha\beta}, \tag{12}$$

где символ $\delta_{\lambda\mu}$, по определению, равен 1, когда $\lambda = \mu$, и равен 0, когда $\lambda \neq \mu$.

Посмотрим теперь, как запишется произведение любых двух элементов A и B нашей алгебры, т. е. вычислим

$$\begin{pmatrix} a_{11}i_{11} + \ldots + a_{1n}i_{1n} + \\ + a_{21}i_{21} + \ldots + a_{2n}i_{2n} + \\ \ldots\ldots\ldots\ldots \\ + a_{n1}i_{n1} + \ldots + a_{nn}i_{nn} \end{pmatrix} \begin{pmatrix} b_{11}i_{11} + \ldots + b_{1n}i_{1n} + \\ + b_{21}i_{21} + \ldots + b_{2n}i_{2n} + \\ \ldots\ldots\ldots\ldots \\ + b_{n1}i_{n1} + \ldots + b_{nn}i_{nn} \end{pmatrix}.$$

В результате должен получиться некоторый элемент C:

$$C = \begin{pmatrix} c_{11}i_{11} + c_{12}i_{12} + \ldots + c_{1n}i_{1n} + \\ + c_{21}i_{21} + c_{22}i_{22} + \ldots + c_{2n}i_{2n} + \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ + c_{n1}i_{n1} + c_{n2}i_{n2} + \ldots + c_{nn}i_{nn} \end{pmatrix}.$$

Рассмотрим произвольное слагаемое $c_{\alpha\beta}i_{\alpha\beta}$ в составе C. Как показывает таблица умножения (11), это слагаемое возникает только от умножения

$a_{\alpha 1}i_{\alpha 1}$ на $b_{1\beta}i_{1\beta}$, $a_{\alpha 2}i_{\alpha 2}$ на $b_{2\beta}i_{2\beta}$, ..., $a_{\alpha n}i_{\alpha n}$ на $b_{n\beta}i_{n\beta}$,

следовательно, оно равняется

$$(a_{\alpha 1}b_{1\beta} + a_{\alpha 2}b_{2\beta} + \ldots + a_{\alpha n}b_{n\beta})\, i_{\alpha\beta}.$$

Итак,

$$c_{\alpha\beta} = a_{\alpha 1}b_{1\beta} + a_{\alpha 2}b_{2\beta} + \ldots + a_{\alpha n}b_{n\beta}.$$

Запомнить эту формулу совсем нетрудно: *нужно взять α-ю строку матрицы A:*

$$a_{\alpha 1}\ a_{\alpha 2}\ \ldots\ a_{\alpha n}$$

и β-й столбец матрицы B:

$$\begin{matrix} b_{1\beta} \\ b_{2\beta} \\ \ldots \\ b_{n\beta}, \end{matrix}$$

затем каждое число строки умножить на соответствующее число столбца и все такие произведения сложить; в итоге получится число $c_{\alpha\beta}$ из матрицы C.

Правило, которое мы сейчас установили, позволяет для любых двух матриц A и B построить третью матрицу C; естественно называть ее *произведением матриц A и B*. Таким образом, чтобы перемножить элементы A и B нашей алгебры, нужно найти произведение соответствующих матриц A и B.

В качестве примера найдем произведение матриц

$$A=\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix} \quad \text{и} \quad B=\begin{pmatrix}6 & -4\\ -3 & 3\end{pmatrix}.$$

Имеем

$$AB=\begin{pmatrix}1\cdot 6+2\cdot(-3) & 1\cdot(-4)+2\cdot 3\\ 3\cdot 6+4\cdot(-3) & 3\cdot(-4)+4\cdot 3\end{pmatrix}=\begin{pmatrix}0 & 2\\ 6 & 0\end{pmatrix}.$$

Возникающее таким путем умножение матриц играет в математике чрезвычайно важную роль. Рамки настоящей книжки не позволяют нам заняться более подробным изучением этой операции. Ограничимся только установлением одного важного свойства умножения матриц: покажем, что *умножение матриц ассоциативно* или, по-другому, — *алгебра матриц является ассоциативной алгеброй.*

Для доказательства достаточно проверить, что равенство $(AB)C = A(BC)$ справедливо, когда в качестве A, B и C берутся любые три «мнимые единицы» алгебры матриц (см. аналогичное рассуждение при доказательстве ассоциативности умножения кватернионов в § 3). Иначе говоря, нужно проверить, что

$$(i_{\alpha\lambda}i_{\mu\beta})\,i_{\nu\gamma}=i_{\alpha\lambda}\,(i_{\mu\beta}i_{\nu\gamma}).$$

Но левая часть согласно (12) равна $(\delta_{\lambda\mu}i_{\alpha\beta})\,i_{\nu\gamma}$ или, снова в силу (12), равна $\delta_{\lambda\mu}\delta_{\beta\nu}i_{\alpha\gamma}$. Аналогично находится правая часть: она равна $i_{\alpha\lambda}(\delta_{\beta\nu}i_{\mu\gamma})$ или $\delta_{\beta\nu}\delta_{\lambda\mu}i_{\alpha\gamma}$. В обоих случаях получается один и тот же результат.

7°. Характеристические свойства умножения в произвольной алгебре*). Из определения алгебры непосредственно вытекают такие свойства операции

*) Содержание этого пункта носит вспомогательный характер и понадобится нам только в §§ 16 и 18.

умножения:

1) $(a+b)c = ac + bc$, $a(b+c) = ab + ac$,
2) $ka \cdot b = k(ab)$, $a \cdot kb = k(ab)$.

Эти свойства являются в некотором смысле *определяющими* для операции умножения. Точнее, имеет место следующее предложение.

Пусть в множестве $\mathcal{A}$ всех выражений вида

$$a_1 i_1 + a_2 i_2 + \ldots + a_n i_n$$

введены: операция (3) *умножения на числа, операция* (4) *сложения, а также некоторая операция**) $a \circ b$, *обладающая указанными выше свойствами* 1) *и* 2):

$$(a+b) \circ c = a \circ c + b \circ c, \qquad a \circ (b+c) = a \circ b + a \circ c,$$
$$ka \circ b = k(a \circ b), \qquad a \circ kb = k(a \circ b).$$

Тогда множество $\mathcal{A}$ есть алгебра, в которой роль операции умножения играет $a \circ b$.

Чтобы доказать это предложение, мы должны проверить, что операция $a \circ b$ есть умножение в том смысле, как об этом говорится в определении алгебры.

Рассмотрим выражение $i_\alpha \circ i_\beta$. Это — некоторый элемент множества $\mathcal{A}$, т. е.

$$i_\alpha \circ i_\beta = p_{\alpha\beta,1} i_1 + p_{\alpha\beta,2} i_2 + \ldots + p_{\alpha\beta,n} i_n. \qquad (13)$$

Из свойств 1) и 2) следует, что

$$a \circ b = (a_1 i_1 + \ldots + a_n i_n) \circ (b_1 i_1 + \ldots + b_n i_n) \overset{!}{=}$$
$$\overset{!}{=} \sum_{\alpha,\beta} [(a_\alpha i_\alpha) \circ (b_\beta i_\beta)] \overset{!!}{=} \sum_{\alpha,\beta} a_\alpha b_\beta (i_\alpha \circ i_\beta)$$

(в равенстве, помеченном !, мы воспользовались свойством 1), в равенстве !! использовали 2)); после этого для вычисления $a \circ b$ остается только вместо $i_\alpha \circ i_\beta$ подставить соответствующий элемент (13), умножить число $a_\alpha b_\beta$ на этот элемент, затем привести подобные члены. Но это — в точности та самая процедура, с помощью которой определяется умножение элементов в произвольной алгебре $\mathcal{A}$.

---

*) В этом месте слова «задана некоторая операция» означают только тот факт, что каждым двум элементам a и b ставится в соответствие третий элемент, обозначаемый $a \circ b$.

n-МЕРНЫЕ ВЕКТОРЫ

Обратимся еще раз к определению алгебры размерности n. В этом определении наиболее сложным моментом является, бесспорно, наличие операции умножения. Останется ли хоть что-нибудь, если отвлечься от этого свойства? Легко видеть, что останется, хотя и не очень много: останется совокупность элементов, однозначно представимых в виде

$$a_1 i_1 + a_2 i_2 + \ldots + a_n i_n,$$

с естественным правилом сложения элементов друг с другом

$$(a_1 i_1 + a_2 i_2 + \ldots + a_n i_n) + (b_1 i_1 + b_2 i_2 + \ldots + b_n i_n) = \\ = (a_1 + b_1) i_1 + (a_2 + b_2) i_2 + \ldots + (a_n + b_n) i_n$$

и со столь же естественным правилом умножения элемента на действительное число:

$$k(a_1 i_1 + a_2 i_2 + \ldots + a_n i_n) = k a_1 i_1 + k a_2 i_2 + \ldots + k a_n i_n.$$

Можно ли, базируясь только на этом материале, развить сколько-нибудь содержательную теорию? Оказывается, что можно. Больше того, существует целый раздел математики, в основе которого лежат только указанные выше операции. Этот раздел называется *линейной алгеброй*; он весьма богат содержанием и используется часто как в самой математике, так и в ее многочисленных приложениях. В этой главе мы ознакомим читателя с некоторыми сведениями из линейной алгебры. Они составят ту основу, на которой будет продолжено изучение теории алгебр в гл. 3.

§ 8. n-мерное векторное пространство A_n

1°. Основные определения. Определение 1. Назовем *n-мерным вектором* объект вида

$$a_1 i_1 + a_2 i_2 + \ldots + a_n i_n, \tag{1}$$

где $a_1, a_2, \ldots, a_n$—произвольные действительные числа, а

$$i_1, i_2, \ldots, i_n$$

— просто n различных символов, которым не приписывается никакого специального смысла.

Поясним, почему выражение (1) названо «вектором». Дело в том, что при $n = 2$ получается выражение вида

$$a_1 i_1 + a_2 i_2, \tag{2}$$

и если истолковывать i_1, i_2 как два фиксированных вектора на обычной плоскости, то написанному выше выражению тоже будет соответствовать некоторый вектор на плоскости *) (рис. 10); больше того, если векторы i_1, i_2 не лежат на одной прямой, то в таком виде может быть записан — и притом однозначно — любой вектор на плоскости.

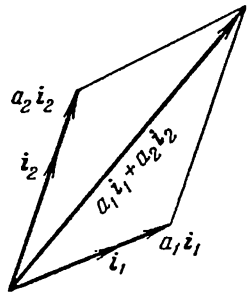


Рис. 10.

Определение 2. Два n-мерных вектора

$$a_1 i_1 + a_2 i_2 + \ldots + a_n i_n$$

и

$$b_1 i_1 + b_2 i_2 + \ldots + b_n i_n$$

считаются *равными* тогда и только тогда, когда

$$a_1 = b_1, \quad a_2 = b_2, \ldots, a_n = b_n.$$

Мотивом к такому определению служит уже упомянутый выше факт, а именно: однозначность представления любого вектора на плоскости в форме (2), если «базисные» векторы i_1, i_2 выбраны не лежащими на одной прямой.

*) Мы исходим из обычного геометрического понимания суммы векторов и произведения вектора на число. Напомним, что сумма векторов определяется по «правилу параллелограмма», а умножение вектора на число k — это растяжение его в $|k|$ раз с последующим изменением направления на противоположное, если $k < 0$.

Определение 3. Сложение n-мерных векторов производится по правилу

$$(a_1\boldsymbol{i}_1 + \ldots + a_n\boldsymbol{i}_n) + (b_1\boldsymbol{i}_1 + \ldots + b_n\boldsymbol{i}_n) = \\ = (a_1 + b_1)\boldsymbol{i}_1 + \ldots + (a_n + b_n)\boldsymbol{i}_n,$$

а умножение n-мерного вектора на действительное число — по правилу

$$k(a_1\boldsymbol{i}_1 + a_2\boldsymbol{i}_2 + \ldots + a_n\boldsymbol{i}_n) = ka_1\boldsymbol{i}_1 + ka_2\boldsymbol{i}_2 + \ldots + ka_n\boldsymbol{i}_n.$$

И это определение, разумеется, навеяно аналогией с геометрическими векторами.

Для сокращенного обозначения n-мерных векторов мы будем пользоваться полужирными латинскими буквами: $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ и т. д. Равенство векторов $\boldsymbol{a}$ и $\boldsymbol{b}$ записывается обычным образом:

$$\boldsymbol{a} = \boldsymbol{b}.$$

Легко видеть, что определенное выше сложение векторов обладает свойствами

$$\boldsymbol{a} + \boldsymbol{b} = \boldsymbol{b} + \boldsymbol{a} \qquad \text{(коммутативность)},$$
$$(\boldsymbol{a} + \boldsymbol{b}) + \boldsymbol{c} = \boldsymbol{a} + (\boldsymbol{b} + \boldsymbol{c}) \qquad \text{(ассоциативность)},$$

а для умножения вектора на число справедливы следующие соотношения:

$$k(l\boldsymbol{a}) = (kl)\boldsymbol{a},$$
$$(k + l)\boldsymbol{a} = k\boldsymbol{a} + l\boldsymbol{a}.$$

Совокупность всех n-мерных векторов будем называть *n-мерным векторным пространством* и обозначать A_n.

Вектор вида

$$0\boldsymbol{i}_1 + 0\boldsymbol{i}_2 + \ldots + 0\boldsymbol{i}_n$$

называется *нулевым вектором* и обозначается $\mathbf{0}$. Очевидно,

$$\boldsymbol{a} + \mathbf{0} = \boldsymbol{a}$$

и

$$0\boldsymbol{a} = \mathbf{0}$$

для любого вектора $\boldsymbol{a}$. В дальнейшем нулевой вектор мы будем называть просто нулем.

2°. Понятие линейной зависимости. Обычно при изучении какого-либо вопроса приходится иметь дело не

с одним отдельным вектором, а с целой системой n-мерных векторов. В этом случае их обозначают, как правило, одной и той же буквой (скажем, a) с различными номерами.

Пример.

$$\begin{aligned} a_1 &= -5i_1 + 3i_2 + 5i_3 + 3i_4, \\ a_2 &= -i_1 + i_2 + 4i_3 + 3i_4, \\ a_3 &= i_1 + 0i_2 + 3i_3 - 2i_4 \end{aligned} \qquad (3)$$

— система трех 4-мерных векторов.

Пусть

$$a_1, a_2, \ldots, a_m$$

— какая-либо система n-мерных векторов. Возьмем произвольные числа

$$k_1, k_2, \ldots, k_m$$

и составим вектор

$$a = k_1a_1 + k_2a_2 + \ldots + k_ma_m.$$

Любой вектор a такого вида называется *линейной комбинацией* данных векторов $a_1, a_2, \ldots, a_m$, а числа $k_1, k_2, \ldots, k_m$ — *коэффициентами* этой линейной комбинации.

Пример. Найти линейную комбинацию

$$a_1 - 3a_2 + 2a_3$$

векторов a_1, a_2, a_3 из приведенной выше системы (3).

Складывая векторы

$$\begin{aligned} a_1 &= -5i_1 + 3i_2 + 5i_3 + 3i_4, \\ -3a_2 &= 3i_1 - 3i_2 - 12i_3 - 9i_4, \\ 2a_3 &= 2i_1 + 0i_2 + 6i_3 - 4i_4, \end{aligned}$$

получаем

$$a_1 - 3a_2 + 2a_3 = 0i_1 + 0i_2 - 1i_3 - 10i_4.$$

Если вектор a является линейной комбинацией векторов $a_1, a_2, \ldots, a_m$, то говорят, что

«a *линейно выражается через* $a_1, a_2, \ldots, a_m$»,

«a *разлагается по* $a_1, a_2, \ldots, a_m$».

Мы будем чаще всего пользоваться последним из указанных выражений.

Введем еще одно важное определение.

Определение 4. Система векторов

$$a_1, a_2, \ldots, a_p \tag{4}$$

называется *линейно зависимой*, если некоторая линейная комбинация этих векторов равна нулевому вектору:

$$s_1a_1 + s_2a_2 + \ldots + s_pa_p = 0, \tag{5}$$

причем хотя бы один из коэффициентов $s_1, s_2, \ldots, s_p$ отличен от нуля. В противном случае (т. е. если не существует линейной комбинации такого рода) система (4) называется *линейно независимой*.

Из определения непосредственно вытекает, что система, состоящая из одного вектора, линейно зависима только в том случае, когда этот вектор — нулевой (действительно, из $s_1a_1 = 0$ и $s_1 \neq 0$ следует $a_1 = 0$).

В случае системы из двух векторов линейная зависимость означает, что найдутся числа s_1 и s_2, из которых хотя бы одно отлично от нуля, такие, что

$$s_1a_1 + s_2a_2 = 0.$$

Пусть, например, $s_1 \neq 0$. Тогда из написанного равенства следует

$$a_1 = ka_2$$

$\left(\text{где } k = -\frac{s_2}{s_1}\right)$. Два вектора, связанные такой зависимостью, называются *пропорциональными*.

Пусть теперь дана линейно зависимая система из любого числа p векторов. Предположим, для определенности, что в равенстве (5) отличен от нуля коэффициент s_1. Тогда из этого равенства следует

$$a_1 = k_2a_2 + k_3a_3 + \ldots + k_pa_p,$$

т. е. вектор a_1 линейно выражается через остальные векторы системы.

Это рассуждение показывает, что линейно зависимая система либо состоит из одного вектора (и тогда это 0), либо один из векторов системы линейно выражается через остальные векторы.

3°. Другое определение линейной зависимости. В дальнейшем нам будет удобнее пользоваться другой формулировкой понятия линейной зависимости: *система* (4) *линейно зависима, если какой-либо из ее векторов*

можно выразить линейно через предшествующие ему векторы системы или же если $a_1 = 0$.

Покажем, что эта формулировка эквивалентна исходной.

В самом деле, если $a_1 = 0$, то система линейно зависима, ибо в этом случае линейная комбинация $1 \cdot a_1 + 0a_2 + \ldots + 0a_p$ равна нулю, причем первый коэффициент отличен от нуля. Если один из векторов системы линейно выражается через предшествующие,

$$a_l = k_1 a_1 + \ldots + k_{l-1} a_{l-1},$$

то в этом случае система также линейно зависима: линейная комбинация $k_1 a_1 + \ldots + k_{i-1} a_{i-1} - 1 a_i + 0 a_{i+1} + \ldots + 0 a_p$ равна нулю, причем коэффициент при a_i отличен от нуля.

Обратно, пусть система линейно зависима, т. е. имеет место (5), причем хотя бы один из коэффициентов $s_1, s_2, \ldots, s_p$ не равен нулю. Рассмотрим последний из отличных от нуля коэффициентов. Если это s_1, то $s_1 a_1 = 0$, следовательно, $a_1 = 0$. Если же указанный коэффициент есть s_i, $i > 1$, то, прибавляя к обеим частям равенства вектор $-s_i a_i$ и умножая обе части на $-\frac{1}{s_i}$, получим равенство вида

$$a_i = k_1 a_1 + \ldots + k_{l-1} a_{l-1},$$

т. е. придем к разложению вектора a_i по предшествующим ему векторам системы.

4°. Первоначальный базис. Вектор

$$1i_1 + 0i_2 + \ldots + 0i_n$$

естественно обозначать коротко через i_1. Таким образом, символ i_1, которому ранее не придавалось никакого специального смысла, теперь отождествляется с одним из векторов. Аналогично вектор

$$0i_1 + 1i_2 + \ldots + 0i_n$$

отождествляем с i_2 и т. д., наконец, вектор

$$0i_1 + 0i_2 + \ldots + 1i_n$$

отождествляем с i_n.

Определенные таким путем векторы

$$i_1, i_2, \ldots, i_n$$

обладают тем свойством, что по ним можно разложить любой вектор из A_n. Действительно, рассмотрим произвольный вектор $a \in A_n$. Он имеет вид формальной суммы

$$a_1 i_1 + a_2 i_2 + \ldots + a_n i_n. \tag{6}$$

Исходя из данных выше определений 2 и 3, можем записать

$$a_1 i_1 + a_2 i_2 + \ldots + a_n i_n = a_1 (1 i_1 + 0 i_2 + \ldots + 0 i_n) +$$
$$+ a_2 (0 i_1 + 1 i_2 + \ldots + 0 i_n) + \ldots + a_n (0 i_1 + 0 i_2 + \ldots + 1 i_n),$$

откуда видно, что вектор a есть линейная комбинация векторов $i_1, i_2, \ldots, i_n$ с коэффициентами $a_1, a_2, \ldots, a_n$. Таким образом, формальную сумму (6) теперь можно рассматривать как настоящую линейную комбинацию.

Векторы $i_1, i_2, \ldots, i_n$ образуют так называемый *базис* пространства A_n. Точный смысл этого слова будет определен в следующем параграфе. Пока же, забегая вперед, заметим, что базисов существует бесконечное множество, и среди них базис $i_1, i_2, \ldots, i_n$ ничем особенным не выделяется.

§ 9. Базис пространства A_n

1° Определение базиса. *Базис пространства* A_n — это система из конечного числа векторов

$$a_1, a_2, \ldots, a_p, \tag{1}$$

обладающая двумя свойствами:

1) любой вектор $a \in A_n$ допускает разложение по ним:

$$a = k_1 a_1 + k_2 a_2 + \ldots + k_p a_p; \tag{2}$$

2) это разложение единственно; иначе говоря, если наряду с (2) имеет место еще одно разложение вектора a:

$$a = l_1 a_1 + l_2 a_2 + \ldots + l_p a_p,$$

то

$$k_1 = l_1, \quad k_2 = l_2, \ldots, \quad k_p = l_p.$$

Докажем одно свойство базиса: *векторы, составляющие базис, линейно независимы.*

В самом деле, допустим, что векторы (1) линейно зависимы. По определению, это означает, что некоторая линейная комбинация этих векторов равна нулю:

$$s_1\boldsymbol{a}_1 + s_2\boldsymbol{a}_2 + \ \ldots\ + s_p\boldsymbol{a}_p = 0, \tag{3}$$

причем среди чисел $s_1, s_2, \ldots, s_p$ хотя бы одно отлично от нуля. Складывая равенства (2) и (3), получим

$$\boldsymbol{a} = (k_1 + s_1)\,\boldsymbol{a}_1 + (k_2 + s_2)\,\boldsymbol{a}_2 + \ \ldots\ + (k_p + s_p)\,\boldsymbol{a}_p,$$

т. е. *другое* разложение $\boldsymbol{a}$ по векторам (1). Но это противоречит определению базиса.

2°. Способ получения других базисов. Примером базиса может служить система

$$\boldsymbol{i}_1,\ \boldsymbol{i}_2,\ \ldots,\ \boldsymbol{i}_n,$$

составленная из первоначальных базисных векторов; условия 1) и 2) для нее, очевидно, выполняются. Но это — отнюдь не единственный базис пространства A_n. Например, из любого базиса можно получить много других с помощью следующих действий:

1. Умножение любого вектора базиса на число, отличное от нуля.

Так, умножая первый из векторов (1) на произвольное число $k \neq 0$, получим новую систему

$$k\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_p, \tag{1'}$$

которая, очевидно, тоже является базисом.

2. Прибавление к одному из базисных векторов другого базисного вектора.

Например, если к $\boldsymbol{a}_1$ прибавить $\boldsymbol{a}_2$, то получим новую систему

$$\boldsymbol{a}_1 + \boldsymbol{a}_2,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_p, \tag{1''}$$

которая тоже является базисом. Действительно, пусть $\boldsymbol{a}$ — произвольный вектор. Тогда имеет место равенство (2), из которого следует, что

$$\boldsymbol{a} = k_1(\boldsymbol{a}_1 + \boldsymbol{a}_2) + (k_2 - k_1)\,\boldsymbol{a}_2 + k_3\boldsymbol{a}_3 + \ \ldots\ + k_p\boldsymbol{a}_p,$$

т. е. что вектор $\boldsymbol{a}$ разлагается по векторам (1″). Далее, из единственности разложения $\boldsymbol{a}$ по базису (1) легко вытекает единственность разложения по (1″). Значит, (1″) есть тоже базис пространства A_n.

Возникает естественный вопрос: как найти все без исключения базисы пространства A_n? Ответ можно было бы мыслить в виде процедуры, позволяющей из какого-либо одного базиса получать все остальные. В определенном смысле такой ответ содержится в следующем предложении, в котором под «элементарными преобразованиями» понимаются определенные выше действия 1 и 2.

От любого базиса к любому другому можно перейти с помощью конечного числа элементарных преобразований.

В частности, если за исходный базис принять базис, составленный из первоначальных базисных векторов $i_1, i_2 \ldots, i_n$, и подвергать его всевозможным элементарным преобразованиям (в любом количестве), то получим все без исключения базисы пространства A_n.

Доказательство сформулированного выше предложения мы не приводим (хотя оно и несложно). Впрочем, для нас представляет интерес не столько само это предложение, сколько одно следствие из него, а именно:

Любой базис пространства A_n состоит из n векторов.

Действительно, в первоначальном базисе $i_1, i_2, \ldots, i_n$ число векторов равно n; но тогда из сказанного выше следует, что и в любом другом базисе число векторов также равно n.

Ниже будет дано независимое доказательство этого предложения.

3°. Число базисных векторов. Нашей ближайшей целью является доказательство следующей теоремы.

Теорема 1. *Любой базис пространства A_n состоит из n векторов.*

Поскольку первоначальный базис $i_1, i_2, \ldots, i_n$ состоит из n векторов, то для нашей цели достаточно показать, что *любые два базиса состоят из одного и того же числа векторов.*

Доказательству этого факта предпошлем одно замечание.

Замечание. Пусть система векторов

$$a_1, a_2, \ldots, a_p$$

такова, что любой вектор a разлагается по ней, — условимся называть такую систему *полной*. Присоединив к полной системе в качестве первого вектора какой-либо вектор $b \neq 0$, получим новую систему

$$b, a_1, a_2, \ldots, a_p,$$

которая будет линейно зависимой (так как в силу полноты имеет место равенство вида $b - k_1a_1 - k_2a_2 - \ldots - k_pa_p = 0$). Согласно 3° § 8 в этой системе найдется вектор a_i, который допускает разложение по одним только предшествующим ему, — условно назовем

такой вектор a_i «лишним». Вычеркнув «лишний» вектор, получим систему снова из p векторов. Покажем, что *эта система, подобно первоначальной системе, будет полной.*

Это почти очевидно. Ведь любой вектор a разлагается по $a_1, a_2, \ldots, a_p$; если в этом разложении заменить «лишний» вектор a_i его разложением по $b, a_1, a_2, \ldots, a_{i-1}$, то придем к разложению вектора a по указанной выше системе из p векторов. Последняя, таким образом, является полной.

Доказательство теоремы теперь проводится в немногих словах. Пусть

$$a_1, a_2, \ldots, a_p \tag{4}$$

и

$$b_1, b_2, \ldots, b_q \tag{5}$$

— два различных базиса пространства A_n. Наша цель — показать, что $p = q$.

Допустим, что $p \neq q$. Для определенности будем считать $p < q$. Присоединим к системе (4) в качестве первого вектора b_1 и полученную таким образом систему освободим от «лишнего» вектора. Мы придем к новой системе

$$b_1, \underbrace{\ldots\ldots\ldots}_{p-1},$$

которая, по доказанному выше, будет полной. Обозначим ее (4′).

Присоединим к системе (4′) в качестве первого вектора b_2 и полученную таким образом систему освободим от «лишнего» вектора. Мы придем к системе

$$b_2, b_1, \underbrace{\ldots\ldots\ldots}_{p-2},$$

которая снова является полной, и т. д.

Заметим, что в роли «лишнего» вектора не может оказаться ни один из присоединяемых векторов $b_1, b_2, \ldots$, ибо эти векторы по условию таковы, что ни один из них не разлагается по остальным (ведь (5) — базис). Таким образом, на каждом шаге вычеркивается один из векторов $a_1, a_2, \ldots, a_p$.

После p шагов все векторы $a_1, a_2, \ldots, a_p$ окажутся вычеркнутыми, и мы придем к системе

$$b_p, b_{p-1}, \ldots, b_2, b_1,$$

которая должна быть полной. Но это невозможно, так как, например, вектор b_{p+1} по этой системе не разлагается.

Итак, предположив, что $q > p$, мы пришли к противоречию. Теорема доказана.

4°. Число векторов, составляющих линейно независимую систему. По доказанному ранее, векторы, образующие любой базис, должны быть линейно независимы. В качестве тривиального следствия отсюда получаем, что в пространстве A_n существуют линейно независимые системы, содержащие n векторов. Но тогда естественно поставить вопрос: можно ли в пространстве A_n построить линейно независимую систему из *большего, чем* n, числа векторов? Покажем, что этого сделать нельзя.

Теорема 2. *Пусть в пространстве* A_n *дана линейно независимая система векторов*

$$a_1, a_2, \ldots, a_p.$$

Тогда $p \leqslant n$. *Если* $p = n$, *то данная система есть базис пространства* A_n.

Доказательство. Обозначим для краткости данную систему через S. Мы будем строить базис пространства A_n, присоединяя к системе S векторы из какого-либо базиса

$$e_1, e_2, \ldots, e_n.$$

Рассмотрим вектор e_1. Если он разлагается по системе S, то оставим его без внимания; если же не разлагается, то добавим его к системе S (в качестве последнего вектора). В обоих случаях полученную систему обозначим S' (она либо совпадает с S, либо получается добавлением к ней вектора e_1).

Затем переходим к вектору e_2. Если он разлагается по системе S', то оставляем его без внимания; если не разлагается, то добавляем его к S'. В обоих случаях полученную систему обозначаем S'' (она либо совпадает с S', либо получается добавлением к ней вектора e_2). Продолжаем так и далее. Перебрав таким образом все векторы $e_1, e_2, \ldots, e_n$, получим систему $S^{(n)}$. Она обладает следующими свойствами:

1. Любой вектор $a \in A_n$ разлагается по ней. Действительно, вектор a разлагается по $e_1, e_2, \ldots, e_n$, а каждый из этих векторов, в свою очередь, разлагается

по векторам системы $S^{(n)}$, как следует из самого способа построения этой системы.

2. Ни один из векторов системы $S^{(n)}$ не разлагается по предыдущим (это опять-таки следует из способа построения $S^{(n)}$). Это означает, что система $S^{(n)}$ линейно независима.

3. Разложение любого вектора a по системе $S^{(n)}$ единственно. В самом деле, если бы существовали два различных разложения для a, то, вычитая из одного другое, мы получили бы линейную зависимость между векторами системы $S^{(n)}$.

Свойства 1 и 3 позволяют сделать заключение, что система $S^{(n)}$ есть базис пространства A_n. По теореме 1 число векторов в этой системе равно n. Поскольку система $S^{(n)}$ содержит исходные векторы $a_1, a_2, \ldots, a_p$, то $p \leqslant n$; в случае $p = n$ исходные векторы сами образуют базис. Теорема доказана.

5°. Одно следствие из теоремы 2, относящееся к алгебрам. В § 7 мы обещали доказать такое предложение: если алгебра $\mathscr{A}$ обладает тем свойством, что из равенства нулю произведения ab следует равенство нулю хотя бы одного из сомножителей a или b, то $\mathscr{A}$ есть алгебра с делением. В тот момент мы не располагали необходимыми средствами, чтобы доказать это предложение. Докажем его теперь.

Пусть требуется решить уравнение

$$ax = b, \tag{6}$$

где $a \neq 0$. Выберем в векторном пространстве $\mathscr{A}$ какой-нибудь базис

$$e_1, e_2, \ldots, e_n.$$

Умножая базисные векторы слева на a, получим другие n векторов

$$ae_1, ae_2, \ldots, ae_n. \tag{7}$$

Покажем, что они снова образуют базис.

Согласно теореме 2, достаточно показать, что векторы (7) линейно независимы. Допустим, что это не так. Тогда существуют числа $k_1, k_2, \ldots, k_n$, не равные одновременно нулю и такие, что

$$k_1ae_1 + k_2ae_2 + \ldots + k_nae_n = 0.$$

Отсюда

$$a(k_1e_1 + k_2e_2 + \ldots + k_ne_n) = 0.$$

Так как по предположению из равенства нулю произведения двух элементов следует равенство нулю одного из сомножителей и так как в нашем случае $a \neq 0$, то

$$k_1e_1 + k_2e_2 + \ldots + k_ne_n = 0,$$

что противоречит линейной независимости векторов $e_1, e_2, \ldots, e_n$.

Таким образом, векторы (7) образуют базис. Разлагая по ним вектор b, можем записать

$$b = s_1ae_1 + s_2ae_2 + \ldots + s_nae_n$$

или

$$b = a(s_1e_1 + s_2e_2 + \ldots + s_ne_n).$$

Отсюда видно, что элемент

$$x = s_1e_1 + s_2e_2 + \ldots + s_ne_n$$

является решением уравнения (6). Это решение единственно: если x' — другое решение, то вычитая из равенства $ax = b$ равенство $ax' = b$, получим

$$a(x - x') = 0,$$

откуда следует $x - x' = 0$, т. е. $x = x'$.

Аналогично доказывается существование и единственность решения уравнения

$$xa = b.$$

6°. Координаты вектора в данном базисе. Последний вопрос, которого мы хотим коснуться в этом параграфе, — это вопрос о координатах вектора в данном базисе пространства A_n.

Пусть

$$a_1, a_2, \ldots, a_n$$

— какой-нибудь базис пространства A_n и

$$p = k_1a_1 + k_2a_2 + \ldots + k_na_n$$

— разложение произвольного вектора $p \in A_n$ по этому базису. Тогда числа $k_1, k_2, \ldots, k_n$ называются *координатами вектора p в данном базисе.*

Равенство

$$(k_1a_1 + \ldots + k_na_n) + (l_1a_1 + \ldots + l_na_n) = \\ = (k_1 + l_1)a_1 + \ldots + (k_n + l_n)a_n,$$

вытекающее из свойств сложения векторов и умножения вектора на число, показывает, что при сложении векторов складываются их соответствующие координаты (первая — с первой, вторая — со второй и т. д.). Аналогично, равенство

$$k(k_1a_1 + k_2a_2 + \ldots + k_na_n) = kk_1a_1 + kk_2a_2 + \ldots + kk_na$$

показывает, что при умножении вектора p на число k все его координаты умножаются на это число. Таким образом, *в произвольном базисе* $a_1, a_2, \ldots, a_n$ *правила сложения векторов и умножения вектора на число остаются теми же, что и в первоначальном базисе* $i_1, i_2, \ldots, i_n$.

§ 10. Подпространства

Остановимся коротко на вопросе о *подпространствах* пространства A_n. Так называются множества векторов, обладающие некоторыми специфическими свойствами; благодаря этим свойствам каждое из таких множеств можно рассматривать как самостоятельное пространство A_p, где $p \leqslant n$.

1°. Определение подпространства. Пусть P — некоторое множество векторов из A_n. Условимся называть это множество *подпространством* пространства A_n, если оно обладает следующими свойствами:

1) из $a \in P$ и $b \in P$ следует $a + b \in P$;

2) из $a \in P$ следует $ka \in P$, где k — любое действительное число.

Иначе говоря, подпространство — это такое множество векторов, которое вместе с любыми своими векторами $a, b, c, \ldots$ содержит и все их линейные комбинации $ka + lb + sc + \ldots$

Тривиальным примером подпространства является множество, состоящее из одного лишь нулевого вектора. Это — так называемое *нулевое* подпространство.

Другой тривиальный пример — все пространство A_n. Однако, кроме этих двух крайних случаев, могут быть и другие подпространства. В следующем пункте мы

укажем, как устроено любое подпространство пространства A_n.

2°. Подпространство как самостоятельное векторное пространство. Предположим, что подпространство P — ненулевое. Покажем, что тогда в P можно выбрать систему векторов, аналогичную базису.

Возьмем какой-нибудь вектор $a_1 \in P$, отличный от нуля. Если все векторы из P разлагаются по a_1, то на этом остановимся. Если же в P имеются векторы, не разлагающиеся по a_1, то выберем один из них a_2 и присоединим его к a_1. Если все векторы из P разлагаются по a_1, a_2, то на этом остановимся. Если же в P имеются векторы, не разложимые по a_1, a_2, то выберем один из них a_3 и присоединим его к a_1, a_2 и т. д. Продолжая этот процесс, мы будем последовательно строить векторы

$$a_1, a_2, a_3, \ldots,$$

причем ни один из них не будет разлагаться по предшествующим; таким образом, на каждом шаге будет получаться линейно независимая система векторов. В силу теоремы 2 предыдущего параграфа этот процесс закончится не позднее чем после n шагов. Мы получим тогда линейно независимую систему векторов

$$a_1, a_2, \ldots, a_p \qquad (p \leqslant n), \tag{1}$$

принадлежащих подпространству P и таких, что:

1) любой вектор из P допускает разложение по ним;

2) это разложение единственно. В самом деле, если бы существовали два различных разложения для вектора a, то, вычитая их друг из друга, мы получили бы, что некоторая линейная комбинация $s_1a_1 + s_2a_2 + \ldots + s_pa_p$ равна нулю, причем хотя бы один из коэффициентов $s_1, s_2, \ldots, s_p$ отличен от нуля; это означало бы линейную зависимость системы (1).

Итак, рассматриваемое нами подпространство P состоит из всевозможных векторов вида

$$k_1a_1 + k_2a_2 + \ldots + k_pa_p,$$

причем представление любого вектора $a \in P$ в таком виде единственно. Это позволяет нам рассматривать подпространство P как самостоятельное p-мерное векторное пространство A_p с первоначальными базисными векторами $a_1, a_2, \ldots, a_p$. Естественно, что в этом пространстве справедливы доказанные ранее теоремы, в

частности: любой базис в нем состоит из p векторов. Число p называют *размерностью подпространства* P. Оно, как мы видели, не превосходит n; в случае, когда оно равняется n, система (1) будет базисом всего пространства A_n (см. снова теорему 2 предыдущего параграфа) и, следовательно, P совпадает с A_n.

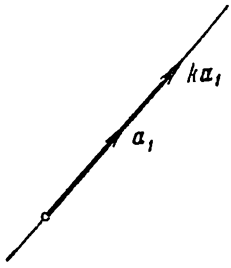


Рис. 11.

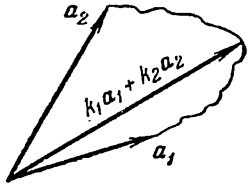


Рис. 12.

Из сказанного выше вытекает одно очевидное следствие, которое мы хотим подчеркнуть особо: *любое подпространство* P *совпадает с множеством всех линейных комбинаций некоторых* p *векторов* $a_1, a_2, \ldots, a_p$.

3°. **Примеры.** Проиллюстрируем понятие подпространства в случае трехмерного векторного пространства A_3.

Пусть P — ненулевое подпространство в A_3. Базис P состоит не более чем из трех векторов, т. е. имеет один из видов:

$$a_1; \quad a_1, a_2; \quad a_1, a_2, a_3.$$

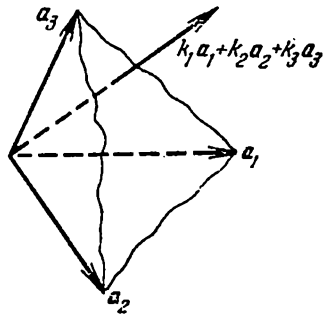


Рис. 13.

В первом случае P состоит из всех векторов вида ka_1, т. е. из всех векторов, пропорциональных a_1 (рис. 11). Во втором случае P есть множество всех векторов вида $k_1a_1 + k_2a_2$, следовательно, P состоит из всех векторов, лежащих в той же плоскости, что и a_1, a_2 (рис. 12). В третьем случае P есть множество всех векторов вида $k_1a_1 + k_2a_2 + k_3a_3$, т. е. всех вообще векторов пространства A_3 (рис. 13).

§ 11. Лемма об однородной системе уравнений

Цель этого параграфа чисто вспомогательная. Мы отвлечемся на короткое время от векторов и обратимся к предмету, казалось бы, не имеющему к ним прямого отношения: *к системам линейных уравнений.* Собственно речь будет идти только об *однородных* уравнениях, а еще точнее — об одной лемме, относящейся к системам таких уравнений. В дальнейшем ссылка на эту лемму поможет нам установить важные предложения.

Как известно, линейное уравнение называется однородным, если его свободный член равен нулю. Несколько отступая от способа записи, принятого в элементарной алгебре, мы будем обозначать неизвестные в уравнении одной и той же буквой x, но с различными номерами: x_1 — первое неизвестное, x_2 — второе и т. д. Тогда линейное однородное уравнение с n неизвестными запишется в виде

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0.$$

Система, состоящая из однородных уравнений, сама называется однородной. В общем виде однородная система из m уравнений с n неизвестными запишется следующим образом:

$$\left.\begin{aligned} &a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0 \text{ — 1-е уравнение}\\ &b_1x_1 + b_2x_2 + \ldots + b_nx_n = 0 \text{ — 2-е уравнение}\\ &\cdots\cdots\cdots\cdots\\ &d_1x_1 + d_2x_2 + \ldots + d_nx_n = 0 \text{ — } m\text{-е уравнение} \end{aligned}\right\} \quad (1)$$

Полагая

$$x_1 = 0,\ x_2 = 0,\ \ldots,\ x_n = 0,$$

мы получим, очевидно, одна из решений однородной системы. Это решение называется *нулевым.* Во многих случаях бывает важно знать, имеет ли данная однородная система еще и ненулевое решение. Частичный ответ на этот вопрос дает следующая лемма.

Лемма. *Однородная система, в которой число уравнений меньше числа неизвестных, всегда имеет ненулевое решение.*

Доказательство будем вести индукцией по m — числу уравнений в системе (1).

Если $m = 1$, то нам дано только одно уравнение, в то время как число неизвестных больше единицы.

Ясно, что у такого уравнения обязательно имеется ненулевое решение.

Предположим, что утверждение теоремы справедливо для систем, состоящих из $m-1$ уравнений, и тогда докажем, что оно остается справедливым для системы из m уравнений.

Итак, пусть нам дана система (1), в которой число m уравнений меньше числа n неизвестных. Если все числа $a_1, b_1, \ldots, d_1$ — коэффициенты при x_1 — равны 0, то система, несомненно, имеет ненулевое решение; например, можно взять

$$x_1 = 1,\ x_2 = 0,\ \ldots,\ x_n = 0.$$

Допустим теперь, что среди указанных коэффициентов имеются отличные от нуля. Поменяв местами, если нужно, первое уравнение с одним из последующих, можно считать, что $a_1 \neq 0$.

Проделаем над системой следующее преобразование: ко второму уравнению прибавим первое, умноженное на $-\frac{b_1}{a_1}$. Получится новая система, очевидно, равносильная исходной. Второе уравнение в ней будет иметь вид

$$b_2'x_2 + \ldots + b_n'x_n = 0$$

(члена с x_1 не будет). Далее проделаем аналогичные преобразования над третьим, четвертым и т. д. (вплоть до m-го) уравнениями системы: к каждому из них прибавим соответствующее кратное первого уравнения. В итоге получится система

$$\left.\begin{array}{l} a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0, \\ \hline \left|\begin{array}{l} b_2'x_2 + \ldots + b_n'x_n = 0, \\ \ldots\ldots\ldots\ldots \\ d_2'x_2 + \ldots + d_n'x_n = 0, \end{array}\right| \end{array}\right\} \qquad (1')$$

равносильная исходной. Часть этой системы, обведенная рамкой, представляет собой однородную систему из $m-1$ уравнений с $n-1$ неизвестными. Так как $m < n$, то

$$m - 1 < n - 1,$$

следовательно, в этой системе число уравнений меньше числа неизвестных. Но для систем, состоящих из $m-1$

уравнений, утверждение леммы справедливо по предположению индукции. Следовательно, система в рамке имеет ненулевое решение

$$x_2 = \alpha_2,\ x_3 = \alpha_3,\ \ldots,\ x_n = \alpha_n.$$

Добавляя к нему значение x_1, определяемое из первого уравнения системы (1′):

$$x_1 = -\frac{1}{a_1}(a_2\alpha_2 + \ldots + a_n\alpha_n),$$

получим ненулевое решение всей системы (1′), а значит, и исходной системы (1). Лемма доказана.

§ 12. Скалярное произведение

В основе всех понятий, изучавшихся в этой главе до сих пор, лежат две операции над векторами: сложение векторов и умножение вектора на число. Между тем, если иметь в виду обычные геометрические векторы *), то круг понятий, связанных с ними, значительно шире: например, каждый вектор имеет длину, существуют перпендикулярные векторы и т. д. Поэтому естественно попытаться найти для n-мерного случая разумный способ введения таких понятий, как длина, перпендикулярность и т. п. Это и будет сделано ниже.

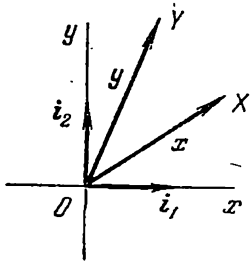


Рис. 14.

1°. Скалярное произведение обычных геометрических векторов. Пусть на плоскости даны два вектора $\boldsymbol{x}$ и $\boldsymbol{y}$, выходящие из начала O прямоугольной системы координат. Координаты первого вектора пусть будут x_1, x_2, второго y_1, y_2. Итак,

$$\boldsymbol{x} = x_1\boldsymbol{i}_1 + x_2\boldsymbol{i}_2,$$
$$\boldsymbol{y} = y_1\boldsymbol{i}_1 + y_2\boldsymbol{i}_2,$$

где $\boldsymbol{i}_1$, $\boldsymbol{i}_2$ — векторы длины 1, имеющие направления координатных осей (рис. 14).

Обозначим концы данных векторов соответственно через X и Y. Точка X имеет координаты x_1, x_2, точка Y — координаты y_1, y_2.

*) Т. е. направленные отрезки на плоскости или в пространстве.

Из формулы для расстояния между двумя точками имеем

$$XY^2 = (y_1 - x_1)^2 + (y_2 - x_2)^2,$$
$$OX^2 = x_1^2 + x_2^2,$$
$$OY^2 = y_1^2 + y_2^2,$$

откуда следует

$$OX^2 + OY^2 - XY^2 = 2(x_1y_1 + x_2y_2). \qquad (1)$$

Из этого равенства легко увидеть (если учесть теорему Пифагора), что необходимым и достаточным условием перпендикулярности $\boldsymbol{x}$ и $\boldsymbol{y}$ является

$$x_1y_1 + x_2y_2 = 0.$$

Заметим, что если это же рассуждение применить к векторам не на плоскости, а в пространстве, то получим условие перпендикулярности в аналогичной форме:

$$x_1y_1 + x_2y_2 + x_3y_3 = 0.$$

Формула (1) наводит на мысль связать с каждой парой векторов $\boldsymbol{x}$ и $\boldsymbol{y}$ на плоскости число

$$x_1y_1 + x_2y_2, \qquad (2)$$

а в пространстве — число

$$x_1y_1 + x_2y_2 + x_3y_3. \qquad (2')$$

Это число в геометрии называют *скалярным произведением* векторов $\boldsymbol{x}$ и $\boldsymbol{y}$ и обозначают $(\boldsymbol{x}, \boldsymbol{y})$.

Заметим, что длина произвольного вектора $\boldsymbol{x}$ выражается через скалярное произведение. А именно, в случае плоскости

$$|\boldsymbol{x}| = \sqrt{x_1^2 + x_2^2},$$

а в случае пространства

$$|\boldsymbol{x}| = \sqrt{x_1^2 + x_2^2 + x_3^2},$$

так что в обоих случаях справедлива формула

$$|\boldsymbol{x}| = \sqrt{(\boldsymbol{x}, \boldsymbol{x})}.$$

2°. Общее определение скалярного произведения. Рассмотренное выше скалярное произведение векторов на плоскости и в пространстве обладает рядом простых свойств. Вот некоторые из них:

1) $(\boldsymbol{x}, \boldsymbol{x}) \geqslant 0$, причем $(\boldsymbol{x}, \boldsymbol{x}) = 0$ только при $\boldsymbol{x} = \mathbf{0}$;

2) $(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{y}, \boldsymbol{x})$;

3) $(\boldsymbol{x}, k\boldsymbol{y}) = k(\boldsymbol{x}, \boldsymbol{y})$, где k — любое действительное число;

4) $(\boldsymbol{x}, \boldsymbol{y} + \boldsymbol{z}) = (\boldsymbol{x}, \boldsymbol{y}) + (\boldsymbol{x}, \boldsymbol{z})$.

Первые три свойства непосредственно вытекают из определения скалярного произведения. Что касается последнего свойства, то его доказательство не намного сложнее. Приведем его для случая пространства:

$$(\boldsymbol{x}, \boldsymbol{y} + \boldsymbol{z}) = x_1(y_1 + z_1) + x_2(y_2 + z_2) + x_3(y_3 + z_3) =$$
$$= (x_1y_1 + x_2y_2 + x_3y_3) + (x_1z_1 + x_2z_2 + x_3z_3) = (\boldsymbol{x}, \boldsymbol{y}) + (\boldsymbol{x}, \boldsymbol{z}).$$

Мы подходим теперь к центральному месту в этом параграфе. При любом обобщении понятия скалярного произведения на n-мерный случай желательно, чтобы свойства 1)—4) сохранили силу. Ввиду этого примем следующее определение.

Определение. Будем говорить, что в n-мерном векторном пространстве A_n задано *скалярное произведение*, если каждым двум векторам $\boldsymbol{x}$ и $\boldsymbol{y}$ сопоставлено некоторое действительное число — обозначим его $(\boldsymbol{x}, \boldsymbol{y})$ — так, что выполнены свойства 1), 2), 3), 4).

Число $(\boldsymbol{x}, \boldsymbol{y})$ будем называть *скалярным произвведением вектора* $\boldsymbol{x}$ *на вектор* $\boldsymbol{y}$.

3°. Один способ введения скалярного произведения. Данное нами определение оставляет открытым вопрос: можно ли хотя бы одним способом ввести в пространстве A_n скалярное произведение? Ответ на него подсказывают выражения (2) и (2′). А именно, выберем в пространстве A_n какой-нибудь базис

$$\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$$

и сопоставим каждым двум векторам $\boldsymbol{x}$ и $\boldsymbol{y}$ число

$$(\boldsymbol{x}, \boldsymbol{y}) = x_1y_1 + x_2y_2 + \ldots + x_ny_n; \qquad (3)$$

здесь $x_1, x_2, \ldots, x_n$ — это координаты вектора $\boldsymbol{x}$, а $y_1, y_2, \ldots, y_n$ — координаты вектора $\boldsymbol{y}$ в выбранном базисе, т. е.

$$\boldsymbol{x} = x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + \ldots + x_n\boldsymbol{a}_n,$$
$$\boldsymbol{y} = y_1\boldsymbol{a}_1 + y_2\boldsymbol{a}_2 + \ldots + y_n\boldsymbol{a}_n.$$

Тогда, как нетрудно показать, все свойства 1)—4) будут выполнены, и следовательно, (x, y) будет скалярным произведением.

Если выбрать другой базис

$$a'_1, a'_2, \ldots, a'_n$$

и сопоставить векторам x и y чйсло

$$(x, y)' = x'_1y'_1 + x'_2y'_2 + \ldots + x'_ny'_n$$

(где $x'_1, x'_2, \ldots, x'_n$ и $y'_1, y'_2, \ldots, y'_n$ суть координаты векторов x и y в новом базисе), то, вообще говоря, равенство

$$(x, y) = (x, y)'$$

выполняться не будет. Отсюда становится ясно, что в пространстве A_n можно ввести много различных скалярных произведений.

В дальнейшем будет показано, что *указанный выше способ введения скалярного произведения является общим: именно, как бы ни выбиралось в пространстве* A_n *скалярное произведение, обязательно найдется такой базис* (*и даже не один*), *в котором имеет место формула* (3).

4°. Длина вектора, ортогональные векторы. После того, как дано определение скалярного произведения, такие понятия, как длина вектора и перпендикулярность двух векторов, вводятся по аналогии с двумерным и трехмерным случаями. А именно, *длину*, или *норму*, n-мерного вектора x мы определяем формулой

$$|x| = \sqrt{(x, x)}$$

(число, стоящее под знаком корня, неотрицательно в силу свойства 1) скалярного произведения); *перпендикулярными*, или *ортогональными*, называем векторы x и y, скалярное произведение которых равно нулю. В этом случае мы пишем

$$x \perp y.$$

Итак,

$x \perp y$ означает, что $(x, y) = 0$.

5°. Выражение скалярного произведения через координаты векторов. Вернемся теперь к определению скалярного произведения и извлечем из основных свойств 1)—4) простейшие следствия.

Прежде всего установим, что справедливы следующие два свойства, дополняющие 3) и 4):

3′) $(kx, y) = k(x, y)$;

4′) $(x + y, z) = (x, z) + (y, z)$.

Свойство 3′) вытекает из цепочки равенств

$$(kx, y) = (y, kx) = k(y, x) = k(x, y),$$

в каждом из которых использовано одно из свойств скалярного произведения. Аналогично доказывается свойство 4′):

$$(x + y, z) = (z, x + y) = (z, x) + (z, y) = (x, z) + (y, z).$$

Комбинируя свойства 3) и 3′), получим

3″) $(kx, ly) = kl(x, y)$.

Далее, из 4) и 4′) сразу же следует, что

$$(x_1 + x_2 + \ldots + x_p, y_1 + y_2 + \ldots + y_q) = \sum_{i, j} (x_i, y_j),$$

т. е. скалярное умножение суммы на сумму подчиняется обычному правилу: каждое слагаемое первой суммы надо умножить на каждое слагаемое второй и результаты сложить. Отсюда, а также из свойства 3″) получается и правило умножения одной линейной комбинации на другую:

$$(k_1x_1 + k_2x_2 + \ldots + k_px_p, l_1y_1 + l_2y_2 + \ldots + l_qy_q) = \sum_{i, j} k_il_j(x_i, y_j). \quad (4)$$

Из этой формулы мы сейчас получим выражение скалярного произведения (x, y) через координаты векторов x и y. Пусть в пространстве A_n выбран некоторый базис

$$a_1, a_2, \ldots, a_n. \quad (5)$$

Рассмотрим два произвольных вектора x и y. Разлагая их по базису (5), получим

$$x = x_1a_1 + x_2a_2 + \ldots + x_na_n,$$
$$y = y_1a_1 + y_2a_2 + \ldots + y_na_n.$$

Теперь для подсчета скалярного произведения (x, y) можно воспользоваться формулой (4):

$$(x, y) = \sum_{i, j} x_i y_j (a_i, a_j).$$

Величины

$$g_{ij} = (a_i, a_j)$$

— это постоянные числа, зависящие только от выбранного базиса. Таким образом, если фиксирован определенный базис, то для скалярного произведения получается выражение

$$(x, y) = \sum_{i, j} g_{ij} x_i y_j. \tag{6}$$

Это — весьма полезный результат; с его помощью мы сейчас докажем ряд важных предложений.

6°. Существование вектора, ортогонального к данным p векторам, $p < n$. Допустим, что вектор y мы зафиксировали, а вектор x хотим выбрать так, чтобы он был ортогонален y, т. е. чтобы было $(x, y) = 0$. Тогда для определения $x_1, x_2, \ldots, x_n$ — координат неизвестного вектора x — получается в силу (6) уравнение

$$\sum_{i, j} g_{ij} x_i y_j = 0.$$

Поскольку g_{ij} и y_j — заданные постоянные числа, то левая часть уравнения после приведения подобных членов принимает вид $a_1 x_1 + a_2 x_2 + \ldots + a_n x_n$; следовательно, полученное уравнение — линейное и однородное относительно неизвестных $x_1, x_2, \ldots, x_n$.

Если нужно, чтобы вектор x был ортогонален не одному вектору y, а нескольким векторам

$$y_1, y_2, \ldots, y_p,$$

то для определения его координат получается уже не одно уравнение, а система из p уравнений. По лемме § 11 такая система заведомо имеет ненулевое решение, если число уравнений меньше числа неизвестных. Отсюда вытекает следующая теорема.

Теорема. *Если в пространстве* A_n *даны векторы*

$$y_1, y_2, \ldots, y_p,$$

причем число этих векторов меньше n, то обязательно существует ненулевой вектор x, ортогональный каждому из данных векторов *).

Эта теорема имеет многочисленные следствия. Мы рассмотрим здесь только одно из них; в дальнейшем оно сыграет важную роль.

Следствие. *Если подпространство* P *пространства* A_n *не совпадает со всем пространством* A_n, *то существует ненулевой вектор* $x \in A_n$, *ортогональный каждому вектору из* P (или, как мы скажем короче, ортогональный всему подпространству P).

Доказательство почти очевидно. Выбираем в P базис из векторов

$$y_1, y_2, \ldots, y_p;$$

поскольку P не совпадает с A_n, то $p < n$. По доказанному, найдется вектор $x \neq 0$, ортогональный каждому из векторов $y_1, y_2, \ldots, y_p$. Но тогда x ортогонален и любой линейной комбинации этих векторов:

$$(x, k_1y_1 + k_2y_2 + \ldots + k_py_p) = \\ = k_1(x, y_1) + k_2(x, y_2) + \ldots + k_p(x, y_p) = 0.$$

Следовательно, x ортогонален любому вектору из P.

7°. Разложение вектора на два составляющих. Мы закончим этот параграф одним утверждением, которое в двумерном и трехмерном случаях выражает геометрически очевидный факт; здесь оно будет доказано для пространства любой размерности n.

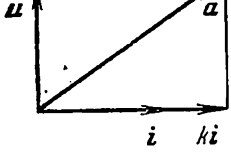


Рис. 15.

Пусть i — какой-либо вектор, отличный от нулевого. Тогда *любой вектор* a *можно разложить на два слагаемых, из которых одно пропорционально* i, *а другое ортогонально* i (рис. 15):

$$a = ki + u, \quad \text{где } u \perp i.$$

Чтобы доказать это утверждение, необходимо проверить, что существует число k, для которого вектор $a - ki$ ортогонален i; тогда, обозначив этот вектор

*) Слово «ненулевой» в формулировке теоремы существенно, поскольку нулевой вектор ортогонален *любому* другому вектору y. Это следует из равенств

$$(0, y) = (0y, y) = 0(y, y) = 0.$$

через u, получим требуемое разложение для a. Итак, необходимо, чтобы

$$(a - ki,\ i) = 0$$

или, что то же,

$$(a,\ i) = k\,(i,\ i).$$

Отсюда сразу находим искомое число k:

$$k = \frac{(a,\ i)}{(i,\ i)}$$

(следует учесть, что $(i, i) \neq 0$, так как вектор i — ненулевой).

§ 13. Ортонормированный базис. Ортогональное преобразование

1°. Определение ортонормированного базиса. Мы уже знаем, что в пространстве A_n существует бесчисленное множество базисов. До введения в A_n скалярного произведения у нас не было причин выделять какие-либо из них особо. Однако с того момента, как возникает скалярное произведение, некоторые базисы начинают играть привилегированную роль. Это — так называемые ортонормированные базисы.

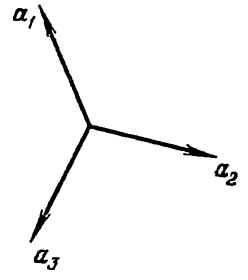


Рис. 16.

Базис

$$a_1,\ a_2,\ \ldots,\ a_n$$

называется *ортонормированным*, если любые два базисных вектора ортогональны друг другу:

$$(a_i,\ a_j) = 0 \qquad (i,\ j = 1,\ \ldots,\ n;\ i \neq j) \tag{1}$$

и длина каждого базисного вектора равна 1:

$$(a_i,\ a_i) = 1 \qquad (i = 1,\ \ldots,\ n). \tag{2}$$

В обычном трехмерном пространстве ортонормированный базис — это любая тройка попарно перпендикулярных единичных векторов (рис. 16).

Заметим, что слово «ортонормированный» происходит от соединения слов «ортогональный» и «нормированный». Вектор a называется *нормированным* или *единичным*, если его длина равна 1.

Ортонормированный базис замечателен тем, что в нем получается особенно простое выражение для скалярного произведения. Воспользуемся формулой

$$(x, y) = \sum_{i,j} x_i y_j (a_i, a_j),$$

доказанной в предыдущем параграфе. Если учесть, что базис — ортонормированный, т. е. что справедливы равенства (1) и (2), то получается сразу

$$(x, y) = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n; \qquad (3)$$

таким образом в ортонормированном базисе скалярное произведение равно сумме произведений одноименных координат (первой — на первую, второй — на вторую и т. д.).

2°. **Существование ортонормированных базисов.** Хотя мы установили важное свойство ортонормированного базиса, но не знаем еще главного: существует ли хотя бы один ортонормированный базис? Сейчас мы докажем, что такой базис существует.

Начнем с такого замечания. Пусть вектор a не является нормированным (однако $a \neq 0$). Тогда из него можно получить нормированный вектор a' по формуле

$$a' = \frac{1}{|a|} a.$$

Действительно,

$$(a', a') = \frac{1}{|a|^2} (a, a) = 1.$$

Переход от a к a' называют *нормированием* вектора a.

Существование ортонормированного базиса легко следует из теоремы, доказанной в предыдущем параграфе. Мы берем любой отличный от нуля вектор b_1; нормируя его, получаем единичный вектор a_1. Далее берем любой отличный от нуля вектор b_2, ортогональный a_1; нормируя его, получаем a_2. Далее выбираем вектор $b_3 \neq 0$, ортогональный a_1 и a_2; нормируя его, получаем вектор a_3 и т. д., пока не дойдем до вектора a_n, ортогонального ранее построенным векторам $a_1, a_2, \ldots, \ldots, a_{n-1}$. Полученная таким путем система

$$a_1, a_2, \ldots, a_n$$

будет базисом в силу теоремы 2 § 9. Действительно, число векторов в системе равно n и, кроме того, эта

система линейно независима: в противном случае, если бы один из векторов системы разлагался по предшествующим, например,

$$a_3 = \alpha a_1 + \beta a_2,$$

то, умножив обе части равенства скалярно на вектор a_3, мы получили бы

$$(a_3, a_3) = 0,$$

что невозможно, ибо $(a_3, a_3) = 1$.

Заметим, что, доказав существование ортонормированного базиса, мы тем самым выполнили обещание, данное в предыдущем параграфе: мы показали, что *существует по крайней мере один базис, в котором скалярное произведение выражается формулой* (3).

3°. Способ получения всех ортонормированных базисов. При изучении ортонормированных базисов возникает ряд интересных вопросов. Вот один из них: как получаются ортонормированные базисы друг из друга? В § 9 мы говорили о том, что любые два базиса пространства A_n получаются один из другого цепочкой элементарных преобразований. Конечно, это предложение справедливо, в частности, и для ортонормированных базисов, но для них оно не представляет особенного интереса: ведь, применив к ортонормированному базису элементарное преобразование, мы получаем, вообще говоря, уже не ортонормированный базис (хотя после нескольких элементарных преобразований может получиться снова ортонормированный базис). Нам хотелось бы, естественно, связать любые два ортонормированных базиса цепочкой таких преобразований, чтобы после каждого из них получался снова ортонормированный базис. Оказывается, это можно сделать следующим образом.

Пусть $a_1, a_2, \ldots, a_n$ — ортонормированный базис. Назовем *элементарным ортопреобразованием* над базисом любое из следующих действий.

1. Умножение любого из базисных векторов на -1. Ясно, что в результате такого преобразования получается снова ортонормированный базис.

2. Замена каких-либо двух векторов a_i, a_j $(i \neq j)$ данного базиса новыми векторами a_i', a_j' по формулам

$$a_i' = \cos\alpha\, a_i - \sin\alpha\, a_j,$$

$$a_j' = \sin\alpha\, a_i + \cos\alpha\, a_j,$$

где α — любое действительное число.

Роль элементарных ортопреобразований вскрывает следующая теорема, которую мы приводим здесь без доказательства.

Теорема. *От любого ортонормированного базиса к любому другому ортонормированному базису можно перейти с помощью конечного числа элементарных ортопреобразований.*

4°. Ортогональные преобразования. С понятием преобразования читатель, вероятно, уже знаком (некоторые виды преобразований изучаются, например, в школьном курсе геометрии). В данном случае речь будет идти о преобразованиях n-мерного векторного пространства A_n.

Мы говорим, что задано *преобразование пространства* A_n, если указано правило, по которому любому вектору $a \in A_n$ отвечает другой вектор $a' \in A_n$.

Наличие такого правила можно отразить следующей записью:

$$a' = F(a),$$

где символ F служит для обозначения того способа, которым a' получается из a.

Преобразование F называется *линейным*, если оно удовлетворяет следующим двум условиям:

1) $F(x + y) = F(x) + F(y)$;

2) $F(kx) = kF(x)$,

где x и y — любые два вектора, а k — любое число. Обозначив векторы $F(x)$ и $F(y)$ через x' и y', можно перефразировать эти условия так: тройку векторов x, y, $x + y$ преобразование F переводит в x', y', $x' + y'$, а пару x, kx — в пару x', kx'. Иначе говоря, преобразование линейно, если оно «не разрушает» ни суммы векторов, ни произведения вектора на число. Разумеется, отсюда следует, что линейное преобразование не разрушает и линейных комбинаций:

$$F(k_1x_1 + k_2x_2 + \ldots + k_px_p) = \\ = k_1F(x_1) + k_2F(x_2) + \ldots + k_pF(x_p).$$

Допустим, что в пространстве A_n введено скалярное произведение. Тогда среди всех линейных преобразований особый интерес приобретают такие, которые «сохраняют» это скалярное произведение, т. е. обладают свойством

$$(F(x), F(y)) = (x, y) \quad \text{для любых} \quad x, y \in A_n.$$

Такие преобразования называются *ортогональными*.

Ясно, что ортогональное преобразование сохраняет и длину любого вектора x, т. е.

$$|F(x)| = |x|.$$

Это следует из того, что длина выражается через

скалярное произведение:

$$|x| = \sqrt{(x, x)}.$$

Сохранение длины любого вектора можно принять за определение ортогонального преобразования. Это видно из того, что скалярное произведение, в свою очередь, выражается через длины. В самом деле, из очевидного равенства

$$(x + y, x + y) = (x, x) + (y, y) + (x, y) + (y, x)$$

вытекает

$$2(x, y) = (x + y, x + y) - (x, x) - (y, y) = \\ = |x + y|^2 - |x|^2 - |y|^2$$

Ортогональные преобразования обладают рядом важных свойств. Укажем одно из них.

Пусть $a_1, a_2, \ldots, a_n$ — ортонормированный базис. Тогда векторы

$$a'_1 = F(a_1), \quad a'_2 = F(a_2), \quad \ldots, \quad a'_n = F(a_n)$$

также образуют ортонормированный базис.

Иначе говоря, *ортогональное преобразование переводит любой ортонормированный базис снова в ортонормированный базис.*

В самом деле, поскольку преобразование F ортогонально, то

$$(a_i, a_j) = (a'_i, a'_j) \qquad (i, j \text{ — любые номера от 1 до } n),$$

следовательно, векторы $a'_1, a'_2, \ldots, a'_n$, подобно $a_1, a_2, \ldots, a_n$, удовлетворяют соотношениям

$$(a'_i, a'_i) = 1, \quad (a'_i, a'_j) = 0 \qquad (\text{при } i \neq j);$$

отсюда вытекает, что они образуют ортонормированный базис (см. рассуждение в конце 2°).

5°. Преобразование, обратное к ортогональному. Прежде всего установим такой факт.

Для ортогонального преобразования F уравнение

$$F(x) = b \tag{4}$$

при любом $b \in A_n$ имеет единственное решение.

Это можно доказать следующим образом. Пусть $a_1, a_2, \ldots, a_n$ — ортонормированный базис. Тогда, как мы знаем, векторы $a'_1 = F(a_1), a'_2 = F(a_2), \ldots, a'_n = F(a_n)$ тоже образуют ортонормированный базис. Разложим по

нему вектор b:

$$b = k_1 a'_1 + k_2 a'_2 + \ldots + k_n a'_n$$

и покажем, что вектор

$$a = k_1 a_1 + k_2 a_2 + \ldots + k_n a_n$$

удовлетворяет уравнению (4). В самом деле, из линейности преобразования F следует, что

$$F(a) = k_1 a'_1 + k_2 a'_2 + \ldots + k_n a'_n = b.$$

Этим доказана разрешимость уравнения (4). То, что решение единственно, доказывается совсем просто: если

$$F(x_1) = b \quad \text{и} \quad F(x_2) = b,$$

то $F(x_1) = F(x_2)$, и значит, $F(x_1 - x_2) = 0$. Но тогда $|x_1 - x_2| = 0$, т. е. $x_1 = x_2$.

Если каждому вектору $b \in A_n$ поставить в соответствие вектор x, являющийся решением уравнения (4), то получим новое преобразование, которое называется *обратным преобразованием* к F и обозначается F^{-1}.

Доказанное выше предложение может быть теперь сформулировано по-другому: *для ортогонального преобразования всегда существует обратное.*

Естественно возникает вопрос: будет ли обратное преобразование снова ортогональным? Докажем, что это так.

Линейность F^{-1} очевидным образом следует из линейности F: если F переводит тройку векторов x, y, $x+y$ в тройку x', y', $x'+y'$, то, обратно, F^{-1} переводит x', y', $x'+y'$ в x, y, $x+y$; если F переводит пару x, kx в пару x', kx', то F^{-1} переводит x', kx' в x, kx. Далее, из равенства

$$(x, y) = (x', y')$$

следует

$$(F^{-1}(x'), F^{-1}(y')) = (x', y').$$

Таким образом, преобразование F^{-1} линейно и сохраняет скалярное произведение. Следовательно, оно ортогональное.

Итак, *преобразование, обратное к ортогональному, снова является ортогональным.*

6°. «Сколько» существует различных ортогональных преобразований? Возникают естественные вопросы: существуют ли вообще ортогональные преобразования и насколько велико их число? Ответить на них нам поможет следующее предложение.

Пусть даны два ортонормированных базиса

$$a_1, a_2, \ldots, a_n \quad \text{и} \quad a'_1, a'_2, \ldots, a'_n.$$

Тогда существует, и притом единственное, ортогональное преобразование, переводящее первый базис во второй.

Искомое преобразование F определяется следующим образом: каждому вектору

$$a = k_1a_1 + k_2a_2 + \ldots + k_na_n$$

сопоставляется вектор

$$F(a) = k_1a'_1 + k_2a'_2 + \ldots + k_na'_n.$$

Покажем, что это преобразование — ортогональное.

Линейность преобразования F очевидна. Остается только проверить, что F сохраняет скалярное произведение. Пусть

$$x = x_1a_1 + \ldots + x_na_n \quad \text{и} \quad y = y_1a_1 + \ldots + y_na_n, \qquad (5)$$

— два произвольных вектора из A_n. Имеем

$$F(x) = x_1a'_1 + \ldots + x_na'_n, \quad F(y) = y_1a'_1 + \ldots + y_na'_n. \qquad (6)$$

Поскольку базис $a_1, \ldots, a_n$ — ортонормированный, то из (5) следует

$$(x, y) = x_1y_1 + x_2y_2 + \ldots + x_ny_n.$$

Но и базис $a'_1, \ldots, a'_n$ — ортонормированный, поэтому из (6) следует

$$(F(x), F(y)) = x_1y_1 + x_2y_2 + \ldots + x_ny_n.$$

Отсюда

$$(x, y) = (F(x), F(y)),$$

т. е. преобразование F — ортогональное.

То, что не может быть другого ортогонального преобразования, переводящего первый базис во второй, легко следует из линейности ортогонального преобразования. Действительно, ввиду линейности искомое преобразование обязано быть таким, как мы его определили.

Из доказанного нами предложения можно вывести такое заключение: между множеством всех ортонормированных базисов и множеством всех ортогональных преобразований можно установить взаимно однозначное соответствие. Для этого следует один из ортонормированных базисов — обозначим его $Б_0$ — зафиксировать, а любому другому ортонормированному базису $Б$ поставить в соответствие то самое ортогональное преобразование, которое переводит $Б_0$ в $Б$. Таким образом, ортогональных преобразований «столько же», сколько существует различных ортонормированных базисов.

ИСКЛЮЧИТЕЛЬНОСТЬ ЧЕТЫРЕХ АЛГЕБР

Среди бесконечного многообразия всех алгебр некоторые алгебры занимают исключительное положение. Это — алгебра $\mathscr{K}$ всех комплексных чисел, алгебра $\mathscr{Q}$ кватернионов и алгебра $\mathscr{O}$ октав. Что же именно отличает эти алгебры от всех остальных? На этот вопрос можно отвечать по-разному, но общий смысл всех ответов сводится к следующему: по сравнению с другими алгебрами указанные три наиболее близки к своей первооснове — алгебре $\mathscr{D}$ всех действительных чисел. Эта близость проявляется, например, в том, что:

1. Алгебры $\mathscr{D}$, $\mathscr{K}$ и $\mathscr{Q}$ — единственные алгебры с делением, в которых умножение обладает свойством ассоциативности. Это предложение, в несколько более точной формулировке, носит название теоремы Фробениуса.

2. Алгебры $\mathscr{D}$, $\mathscr{K}$, $\mathscr{Q}$ и $\mathscr{O}$ — единственные алгебры с делением, в которых справедливы формулы $(uv)v = u(vv)$ и $v(vu) = (vv)u$ (ослабленный вариант ассоциативности, называемый альтернативностью). Это утверждение называется обобщенной теоремой Фробениуса.

3. Алгебры $\mathscr{D}$, $\mathscr{K}$, $\mathscr{Q}$ и $\mathscr{O}$ — единственные алгебры с единицей, в которых можно ввести скалярное произведение так, чтобы выполнялось правило «норма произведения равна произведению норм». Этот факт составляет содержание теоремы Гурвица.

Словом, в иерархии алгебр положение представляется примерно в следующем виде. «Основой основ» служит алгебра действительных чисел. Ее ближайшим соседом является алгебра комплексных чисел, в которой умножение сохраняет все важнейшие свойства умножения действительных чисел: оно коммутативно, ассоциативно, обратимо (иначе говоря — возможно деление)

и для него существует единица. Далее следует алгебра кватернионов — из перечисленных выше свойств в ней теряется только коммутативность умножения. Еще дальше расположена алгебра октав, где ассоциативность заменяется слабым подобием этого свойства — «альтернативностью», но по-прежнему возможно деление и существует единица. Все остальные алгебры не удерживают даже и этих свойств. Конечно, отсюда еще не следует, что остальные алгебры менее интересны или менее важны, — в данном случае речь идет только о большем или меньшем сходстве с алгеброй действительных чисел.

Ко всему сказанному мы можем добавить еще одно замечание. В гл. 1 была поставлена «задача о сумме квадратов», заключающаяся в разыскании всех тождеств определенного типа:

$$(a_1^2 + a_2^2 + \ldots + a_n^2)(b_1^2 + b_2^2 + \ldots + b_n^2) = \\ = \Phi_1^2 + \Phi_2^2 + \ldots + \Phi_n^2 \quad (1)$$

(см. § 3). Исходя из одного упомянутого выше свойства алгебр $\mathcal{D}$, $\mathcal{K}$, $\mathcal{Q}$ и $\mathcal{O}$ (норма произведения равна произведению норм), мы построили в гл. 1 конкретные примеры таких тождеств для $n = 1, 2, 4, 8$. В настоящей главе будет показано, что число n в тождестве (1) может принимать только эти четыре значения; решающую роль в доказательстве этого факта будет играть теорема Гурвица. Таким образом, и в «задаче о сумме квадратов» основными персонажами выступают все те же алгебры $\mathcal{D}$, $\mathcal{K}$, $\mathcal{Q}$ и $\mathcal{O}$.

Эта глава посвящена уточнению и доказательству всех перечисленных выше фактов.

§ 14. Изоморфные алгебры

Согласно определению, данному в § 7, любая алгебра размерности n состоит из элементов, однозначно представимых в виде

$$a_1 i_1 + a_2 i_2 + \ldots + a_n i_n,$$

с естественным законом сложения элементов между собой и умножения их на действительные числа; другими словами, каждая алгебра размерности n есть, прежде всего, n-мерное векторное пространство. Сверх того,

должна быть задана таблица умножения (первоначальных) базисных элементов $i_1, i_2, \ldots, i_n$, т. е. таблица из n^2 соотношений вида

$$i_\alpha i_\beta = k_{\alpha\beta,1} i_1 + k_{\alpha\beta,2} i_2 + \ldots + k_{\alpha\beta,n} i_n \qquad (1)$$
$$(\alpha, \beta = 1, 2, \ldots, n),$$

где $k_{\alpha\beta,\gamma}$ — некоторые действительные числа. После того как указаны правила перемножения базисных элементов, произведение любых двух элементов

$$a_1 i_1 + \ldots + a_n i_n \quad \text{и} \quad b_1 i_1 + \ldots + b_n i_n$$

алгебры производится по обычному правилу умножения суммы на сумму, с последующим учетом соотношений (1).

Можно сказать поэтому, что любая алгебра размерности n — это n-мерное векторное пространство A_n, в котором дополнительно задана таблица умножения базисных элементов — таблица (1).

Казалось бы, отсюда напрашивается вывод, что две алгебры размерности n, определенные *различными* таблицами умножения, следует рассматривать как различные алгебры. Однако такая точка зрения была бы не совсем правильной, и вот почему.

Пусть $\mathcal{A}$ — алгебра размерности n с первоначальным базисом $i_1, i_2, \ldots, i_n$ и таблицей умножения (1). Перейдем в векторном пространстве $\mathcal{A}$ к другому базису $i'_1, i'_2, \ldots, i'_n$; естественно, получим и другую таблицу умножения

$$i'_\alpha i'_\beta = l_{\alpha\beta,1} i'_1 + l_{\alpha\beta,2} i'_2 + \ldots + l_{\alpha\beta,n} i'_n \qquad (2)$$
$$(\alpha, \beta = 1, 2, \ldots, n).$$

Теперь представим себе еще одну алгебру — обозначим ее $\mathcal{A}'$ — с первоначальным базисом $i'_1, i'_2, \ldots, i'_n$ и с таблицей умножения (2). Следует ли рассматривать ее как новую алгебру? Формально, разумеется, это так, но, по существу, $\mathcal{A}'$ есть та же самая алгебра $\mathcal{A}$, только отнесенная к другому базису. Естественно поэтому считать различие между алгебрами $\mathcal{A}$ и $\mathcal{A}'$ несущественным. Такая точка зрения находит свое выражение в понятии изоморфизма.

Определение. Две алгебры одной и той же размерности n называются *подобными* друг другу или

изоморфными, если в них можно выбрать базисы с одинаковыми таблицами умножения.

Разумеется, совпадение таблиц умножения вовсе не предполагает одинаковый выбор обозначений для базисных элементов обоих алгебр; например, базисные элементы первой алгебры могут быть обозначены $c_1, c_2, \ldots, c_n$, а второй, — скажем, $d_1, d_2, \ldots, d_n$. Требуется лишь, чтобы каждое произведение $c_\alpha c_\beta$ разлагалось по $c_1, c_2, \ldots, c_n$ с *точно такими же* коэффициентами, как и произведение $d_\alpha d_\beta$ по $d_1, d_2, \ldots, d_n$. Это означает, что если, например,

$$c_3 c_2 = 3c_1 - 7c_5,$$

то должно быть также

$$d_3 d_2 = 3d_1 - 7d_5.$$

В математике *две изоморфные алгебры не считаются различными: это — как бы два различных экземпляра одной и той же алгебры.* В связи с этим, когда ставится вопрос об отыскании всех алгебр, обладающих каким-либо отличительным свойством, ответ ищется в форме: искомая алгебра изоморфна либо такой-то конкретной алгебре, либо такой-то и т. д.

В гл. 1 мы ввели понятие гиперкомплексной системы, а затем — более широкое понятие алгебры. Соотношение между ними в полной мере может быть вскрыто только теперь, когда мы владеем понятием изоморфизма. Было показано (§ 7), что любая гиперкомплексная система может рассматриваться как алгебра, в которой первый из первоначальных базисных элементов является единицей алгебры:

$$i_1 i_\alpha = i_\alpha i_1 = i_\alpha \qquad \text{для всех } \alpha.$$

Теперь мы можем добавить к этому предложение, в некотором смысле обратное: любая алгебра с единицей изоморфна некоторой гиперкомплексной системе. В самом деле, если дана алгебра с единицей $\mathbf{1}$, то, выбрав в ней новый базис $i'_1, i'_2, \ldots, i'_n$ так, чтобы было $i'_1 = \mathbf{1}$, мы получим таблицу умножения, в которой $i'_1 i'_\alpha = i'_\alpha i'_1 = i'_\alpha$ для всех α, т. е. таблицу умножения в некоторой гиперкомплексной системе $\mathscr{M}$. Отсюда следует, что исходная алгебра изоморфна гиперкомплексной системе $\mathscr{M}$.

В заключение приведем один пример, иллюстрирующий роль понятия изоморфизма. Исходя из результатов, полученных в § 2, мы можем теперь сказать, что любая алгебра размерности 2, обладающая единицей, изоморфна одной из трех гиперкомплексных систем: комплексных, двойных или дуальных чисел. Именно это и есть перевод на точный язык того факта, который в § 2 мы выражали словами «любая система чисел $a + bi$ сводится к одной из трех ...». «Сводится к» означает «изоморфна»!

§ 15. Подалгебры

В гл. 1 мы неоднократно сталкивались с таким явлением, когда одна алгебра является частью другой: например, алгебра действительных чисел является частью алгебры комплексных чисел, последняя является частью алгебры кватернионов; эта алгебра, в свою очередь, входит в алгебру октав и т. п. В подобных случаях вместо слова «часть» употребляют термин «подалгебра».

Определение. Множество $\mathscr{P}$ элементов алгебры $\mathscr{A}$ называется *подалгеброй* алгебры $\mathscr{A}$, если:

1) $\mathscr{P}$ является подпространством векторного пространства $\mathscr{A}$;

2) $\mathscr{P}$ замкнуто относительно умножения в алгебре $\mathscr{A}$, т. е. если $\boldsymbol{a} \in \mathscr{P}$ и $\boldsymbol{b} \in \mathscr{P}$, то $\boldsymbol{ab} \in \mathscr{P}$.

Первое требование равносильно (§ 10) тому, что $\mathscr{P}$ есть множество всех линейных комбинаций

$$k_1\boldsymbol{a}_1 + k_2\boldsymbol{a}_2 + \ldots + k_p\boldsymbol{a}_p$$

некоторых векторов $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_p$. Последние могут быть выбраны линейно независимыми; в этом случае они составляют базис подпространства $\mathscr{P}$ (и число их не превышает n).

Для того, чтобы было выполнено второе требование, фактически достаточно, чтобы всевозможные произведения базисных элементов

$$\boldsymbol{a}_\alpha\boldsymbol{a}_\beta \qquad (\alpha, \beta = 1, 2, \ldots, p)$$

принадлежали снова $\mathscr{P}$, т. е. чтобы имели место равенства

$$\boldsymbol{a}_\alpha\boldsymbol{a}_\beta = k_{\alpha\beta,1}\boldsymbol{a}_1 + k_{\alpha\beta,2}\boldsymbol{a}_2 + \ldots + k_{\alpha\beta,p}\boldsymbol{a}_p \qquad (1)$$
$$(\alpha, \beta = 1, \ldots, p).$$

Из данного выше определения непосредственно ясно, что подалгебра $\mathcal{P}$ может рассматриваться как самостоятельная алгебра с первоначальными базисными элементами $a_1, a_2, \ldots, a_p$ и таблицей умножения (1).

Приведем несколько примеров подалгебр.

1. В алгебре кватернионов подалгеброй является подпространство с базисом $1, j$. Более общий пример: подпространство с базисом $1, q$, где q — какой-либо кватернион, не пропорциональный 1. Любая такая подалгебра изоморфна алгебре комплексных чисел.

2. В алгебре октав подалгеброй является подпространство с базисом $1, i, E, I$. Эта подалгебра изоморфна алгебре кватернионов (в указанном базисе таблица умножения — та же самая, что и в базисе $1, i, j, k$ алгебры кватернионов). Аналогичные примеры: любое подпространство с базисом $1, a, b, ab$, где a и b — любые две мнимые единицы из первоначального базиса $1, i, j, k, E, I, J, K$ алгебры октав.

3. В алгебре матриц данного порядка n подалгеброй является подпространство матриц, у которых все элементы первых k строк (k — фиксированное число) равны нулю. Более сложный пример: подпространство «шахматных» матриц, т. е. матриц, у которых элементы a_{ij}, где $i+j$ — нечетное число, равны нулю. Например, при $n=3$ это будут матрицы вида

$$\begin{pmatrix} * & 0 & * \\ 0 & * & 0 \\ * & 0 & * \end{pmatrix}.$$

Проверку того, что указанные подпространства являются подалгебрами, предоставляем читателю.

§ 16. Перевод «задачи о сумме квадратов» на язык теории алгебр. Нормированные алгебры

Напомним читателю формулировку «задачи о сумме квадратов», поставленной в гл. 1. Требуется выяснить, каким должно быть n и как должны быть выбраны n форм второй степени

$$\Phi_1(x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n),$$
$$\Phi_2(x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\Phi_n(x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n)$$

для того, чтобы было справедливо тождество

$$(x_1^2 + x_2^2 + \ldots + x_n^2)(y_1^2 + y_2^2 + \ldots + y_n^2) = \\ = \Phi_1^2 + \Phi_2^2 + \ldots + \Phi_n^2. \quad (!)$$

Изучение некоторых конкретных алгебр (алгебр комплексных чисел, кватернионов, октав) позволило нам построить в главе I примеры тождеств (!) для $n = 2$, $n = 4$ и $n = 8$. Однако там ничего не было сказано о том, как строится *любое* тождество (!). Этим вопросом мы займемся сейчас.

1°. Связь тождества (!) с некоторой алгеброй $\mathscr{A}$. Прежде всего заметим, что с каждым тождеством (!) связана некоторая алгебра. Эта алгебра определяется следующим образом. Мы рассматриваем n-мерное векторное пространство, элементами которого являются векторы

$$x_1 i_1 + x_2 i_2 + \ldots + x_n i_n. \quad (1)$$

Произведение любых двух элементов этого пространства

$$x = x_1 i_1 + x_2 i_2 + \ldots + x_n i_n$$

и

$$y = y_1 i_1 + y_2 i_2 + \ldots + y_n i_n$$

определяем формулой

$$xy = \Phi_1 i_1 + \Phi_2 i_2 + \ldots + \Phi_n i_n. \quad (2)$$

Ввиду «линейности» форм Φ_1, Φ_2, ..., Φ_n по переменным x_1, x_2, ..., x_n, а также по переменным y_1, y_2, ..., y_n ясно, что выполняется каждое из написанных ниже равенств:

$$kx \cdot y = k(xy), \qquad x \cdot ky = k(xy),$$
$$(x_1 + x_2)y = x_1 y + x_2 y, \quad x(y_1 + y_2) = xy_1 + xy_2.$$

Отсюда следует, что закон умножения (2) действительно определяет некоторую алгебру (см. 7° § 7). Обозначим эту алгебру $\mathscr{A}$. Как следует из сказанного выше, алгебра $\mathscr{A}$ полностью определена, как только задано тождество (!).

2°. Нормированность алгебры $\mathscr{A}$. Посмотрим, какому свойству алгебры $\mathscr{A}$ соответствует тот факт, что $\Phi_1, \Phi_2, \ldots, \Phi_n$ — не просто какие-то формы второй

степени, а такие, для которых справедливо тождество (!).

С этой целью зададим в алгебре $\mathscr{A}$ скалярное произведение (x, y), определив его через координаты векторов x и y в базисе $i_1, i_2, \ldots, i_n$:

$$(x, y) = x_1y_1 + x_2y_2 + \ldots + x_ny_n. \tag{3}$$

В частности,

$$(x, x) = x_1^2 + x_2^2 + \ldots + x_n^2.$$

Заметим, что, определяя скалярное произведение указанным образом, мы тем самым заранее приписываем базису $i_1, i_2, \ldots, i_n$ роль ортонормированного базиса, ибо

$$(i_\alpha, i_\alpha) = 1,$$
$$(i_\alpha, i_\beta) = 0$$

при всех $\alpha, \beta = 1, \ldots, n$, $\alpha \neq \beta$. Для пояснения этих равенств заметим, что у вектора i_α отлична от нуля только α-я координата (она равна 1), а у вектора i_β — только β-я.

Теперь, когда в алгебре $\mathscr{A}$ определено скалярное произведение, можно по-новому истолковать тождество (!). Выражение, стоящее в правой части тождества, как нетрудно заметить, равно (xy, xy) — «скалярному квадрату» элемента xy; левая же часть представляет собой произведение двух «скалярных квадратов»: (x, x) и (y, y). Поэтому вместо (!) можно записать

$$(xy, xy) = (x, x)(y, y). \tag{4}$$

Впрочем, если ввести в рассмотрение норму элемента x, определяемую формулой

$$|x| = \sqrt{(x, x)},$$

то равенство (4) можно, в свою очередь, записать так:

$$|xy| = |x||y| \tag{4'}$$

(норма произведения равна произведению норм).

Примем теперь следующее

Определение. Алгебра $\mathscr{A}$ называется *нормированной*, если в ней можно ввести скалярное произведе-

ние таким образом, что будет выполняться тождество (4).

Примерами нормированных алгебр являются уже известные нам алгебры комплексных чисел, кватернионов и октав. Их нормированность следует из того, что в каждой из этих алгебр справедлива формула (4′); при этом, чтобы все в точности соответствовало определению нормированной алгебры, нужно только указать такое скалярное произведение (x, y), для которого выполнялось бы равенство $|x| = \sqrt{(x, x)}$. В случае алгебры комплексных чисел такое скалярное произведение определяется формулой

$$(z, z') = x_1y_1 + x_2y_2,$$

где $z = x_1 + y_1i$, $z' = x_2 + y_2i$, для алгебры кватернионов

$$(q, q') = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4,$$

где $q = x_1 + x_2i + x_3j + x_4k$, $q' = y_1 + y_2i + y_3j + y_4k$; аналогичным образом определяется скалярное произведение в алгебре октав.

3°. **Заключение.** Итак, мы доказали, что каждому тождеству (!) можно сопоставить некоторую нормированную алгебру $\mathscr{A}$. Умножение любых двух элементов $x = x_1i_1 + \ldots + x_ni_n$, $y = y_1i_1 + \ldots + y_ni_n$ в этой алгебре определено по формуле

$$xy = \Phi_1i_1 + \ldots + \Phi_ni_n, \tag{5}$$

а скалярное произведение — по формуле

$$(x, y) = x_1y_1 + x_2y_2 + \ldots + x_ny_n.$$

В алгебре $\mathscr{A}$ элементы $i_1, i_2, \ldots, i_n$ образуют ортонормированный базис; при этом тождество (!) есть не что иное, как условие нормированности алгебры $\mathscr{A}$, записанное в этом базисе.

Легко видеть, что справедливо и обратное утверждение, а именно: если дана произвольная нормированная алгебра $\mathscr{A}$ и в ней выбран любой ортонормированный базис $i_1, i_2, \ldots, i_n$, то, записав закон умножения в этом базисе, получим n форм $\Phi_1, \Phi_2, \ldots, \Phi_n$, а записав условие нормированности алгебры $\mathscr{A}$, получим тождество (!) с этими формами в правой части.

Подводя итог сказанному, приходим к такому заключению.

Все наборы форм $\Phi_1, \Phi_2, \ldots, \Phi_n$, *удовлетворяющие тождеству* (!), *могут быть получены следующим путем. Нужно взять любую нормированную алгебру* $\mathcal{A}$ *и в ней произвольный ортонормированный базис* $i_1, i_2, \ldots, i_n$, *затем записать закон умножения алгебры* $\mathcal{A}$ *в виде* (5).

Отсюда видно, что задача перечисления всех тождеств (!) сводится к двум задачам:

1) разысканию всех нормированных алгебр;

2) записи закона умножения для каждой из таких алгебр в каждом из ее ортонормированных базисов.

Первую из этих задач мы рассмотрим в ближайших двух параграфах. На основе ее решения будет получено обозрение всех тождеств (!).

§ 17. Нормированные алгебры с единицей. Теорема Гурвица

1°. Формулировка теоремы Гурвица. В предыдущем параграфе, обсуждая «задачу о сумме квадратов», мы пришли к необходимости найти все возможные нормированные алгебры. Ниже будет доказана теорема, впервые установленная немецким математиком А. Гурвицем в 1898 г. Она хотя и не дает еще полного перечисления всех нормированных алгебр, но все же снимает основную долю трудностей, связанных с решением этой задачи.

Теорема Гурвица. *Любая нормированная алгебра с единицей изоморфна одной из четырех алгебр: действительных чисел, комплексных чисел, кватернионов или октав.*

Условие, что алгебра имеет единицу, в формулировке теоремы не может быть опущено. Как мы увидим дальше, существуют нормированные алгебры, не содержащие единицы; такие алгебры не могут быть изоморфны ни одной из четырех указанных в теореме, поскольку в каждой из этих четырех алгебр единица имеется.

Итак, пусть $\mathcal{A}$ — нормированная алгебра с единицей. Напомним, что мы условились называть алгебру нормированной, если в ней можно ввести скалярное произведение со следующим свойством:

$$(ab, ab) = (a, a)(b, b). \qquad (1)$$

Приступая к доказательству теоремы, мы хотим заранее оговорить, что оно будет довольно длинным. Поэтому вначале мы изложим общую схему, раскрывающую идеи доказательства, после чего заполним «дыры» в проведенных рассуждениях.

2°. Набросок доказательства. Обозначим единицу алгебры $\mathcal{A}$ через $\mathbf{1}$. Каждый элемент $a \in \mathcal{A}$ однозначно представляется в виде суммы двух слагаемых *), из которых одно пропорционально $\mathbf{1}$, а другое ортогонально $\mathbf{1}$:

$$a = k\mathbf{1} + a',$$

где k — действительное число, а $a' \perp \mathbf{1}$. Введем в алгебре следующую операцию сопряжения: элемент, сопряженный a, есть

$$\bar{a} = k\mathbf{1} - a'.$$

В частности, если элемент a пропорционален $\mathbf{1}$, то $\bar{a} = a$; если же a ортогонален $\mathbf{1}$, то $\bar{a} = -a$. Очевидно также, что

$$\bar{\bar{a}} = a$$

и

$$\overline{a + b} = \bar{a} + \bar{b}.$$

Теперь, когда в алгебре $\mathcal{A}$ введено сопряжение, можно приступить к изложению идей, лежащих в основе доказательства теоремы.

Пусть $\mathcal{U}$ — *какая-нибудь подалгебра алгебры* $\mathcal{A}$, *содержащая* $\mathbf{1}$ *и не совпадающая со всей алгеброй.* Выберем в $\mathcal{U}$ базис из элементов $\mathbf{1}, i_1, i_2, \ldots, i_n$, где $i_1, i_2, \ldots, i_n$ ортогональны $\mathbf{1}$, тогда для любого элемента $a_0 + a_1 i_1 + \ldots + a_n i_n$ из $\mathcal{U}$ сопряженный будет $a_0 - a_1 i_1 - \ldots - a_n i_n$. Отсюда видно, что если элемент u принадлежит $\mathcal{U}$, то и сопряженный ему элемент $\bar{u}$ также принадлежит $\mathcal{U}$.

Согласно теореме § 12, существует ненулевой вектор, ортогональный $\mathcal{U}$; умножая его на подходящее число, получим *единичный вектор* e, *ортогональный* $\mathcal{U}$. Будет показано, что множество элементов вида

$$u_1 + u_2 e \qquad (u_1 \in \mathcal{U},\ u_2 \in \mathcal{U}) \tag{2}$$

*) В этом месте, а также в последующих рассуждениях мы опираемся на общие свойства скалярного произведения, рассмотренные в § 12.

замкнуто относительно умножения, т. е. снова образует подалгебру. Обозначим последнюю $\mathcal{U} + \mathcal{U}e$. Мы докажем, что:

I) представление любого элемента из $\mathcal{U} + \mathcal{U}e$ в виде (2) возможно лишь единственным образом;

II) для произведения элементов вида (2) справедлива формула

$$(u_1 + u_2 e)(v_1 + v_2 e) = (u_1 v_1 - \bar{v}_2 u_2) + (v_2 u_1 + u_2 \bar{v}_1) e. \quad (3)$$

Сопоставив эти факты с процедурой удвоения, описанной в § 6, мы приходим к следующему заключению: *подалгебра $\mathcal{U} + \mathcal{U}e$ изоморфна удвоенной подалгебре $\mathcal{U}$.*

Теперь основные трудности в доказательстве теоремы остаются позади. Прежде чем перейти к завершающему этапу доказательства, сделаем одно замечание по поводу сопряжения в алгебре $\mathcal{A}$.

Поскольку алгебра $\mathcal{A}$ содержит единицу, то в ней имеется подалгебра, состоящая из элементов вида $k\mathbf{1}$. Эта подалгебра изоморфна алгебре действительных чисел; обозначим ее $\mathcal{D}$. Если в предыдущих рассуждениях в качестве $\mathcal{U}$ взять подалгебру $\mathcal{D}$, то e будет любой вектор длины 1, ортогональный $\mathbf{1}$. Из формулы (3) тогда следует, что

$$e^2 = (0 + 1e)(0 + 1e) = -1.$$

Отсюда можно сделать заключение, что квадрат любого вектора a', ортогонального $\mathbf{1}$, равен $\lambda\mathbf{1}$, где $\lambda \leqslant 0$. Легко доказать и обратное: если квадрат какого-либо элемента равен $\lambda\mathbf{1}$, где $\lambda \leqslant 0$, то этот элемент ортогонален $\mathbf{1}$ *). Таким образом, элементы, ортогональные $\mathbf{1}$, и только они характеризуются тем, что их квадраты равны $\lambda\mathbf{1}$, где $\lambda \leqslant 0$. Это позволяет нам описать по-другому сопряжение в алгебре $\mathcal{A}$: *для произвольного элемента $a \in \mathcal{A}$ берется его единственное представление в виде*

$$k\mathbf{1} + a', \quad \text{где} \quad a'^2 = \lambda\mathbf{1}, \quad \lambda \leqslant 0,$$

тогда $\bar{a} = k\mathbf{1} - a'$.

*) Действительно, квадрат любого элемента, не ортогонального $\mathbf{1}$, т. е. элемента вида $a = k\mathbf{1} + a'$, где $k \neq 0$, $a' \perp \mathbf{1}$, равен

$$(k\mathbf{1} + a')(k\mathbf{1} + a') = k^2\mathbf{1} + a'^2 + 2ka' = k^2\mathbf{1} + \mu\mathbf{1} + 2ka'.$$

Если это выражение пропорционально $\mathbf{1}$, то $a' = 0$, следовательно, $a = k\mathbf{1}$, но квадрат такого элемента не может равняться $\lambda\mathbf{1}$, где $\lambda \leqslant 0$.

Перейдем к завершающей части доказательства; она представляет собой следующее весьма прозрачное рассуждение.

Рассмотрим снова подалгебру $\mathscr{D}$. Если она не совпадает со всей алгеброй $\mathscr{A}$, то найдется единичный вектор e, ортогональный $\mathscr{D}$. Рассмотрим тогда подалгебру $\mathscr{K} = \mathscr{D} + \mathscr{D}e$. Она является удвоением $\mathscr{D}$ и, следовательно, изоморфна алгебре комплексных чисел. Из того, что сказано выше о сопряжении в алгебре $\mathscr{A}$, следует, что для элементов из $\mathscr{K}$ сопряжение совпадает с обычным сопряжением комплексных чисел.

Если подалгебра $\mathscr{K}$ не совпадает со всей алгеброй $\mathscr{A}$, то опять-таки найдется единичный вектор e', ортогональный $\mathscr{K}$. Рассмотрим тогда подалгебру $\mathscr{Q} = \mathscr{K} + \mathscr{K}e'$, являющуюся удвоением $\mathscr{K}$. Она изоморфна алгебре кватернионов. Из данной выше характеристики сопряжения в алгебре $\mathscr{A}$ снова следует, что для элементов из $\mathscr{Q}$ сопряжение совпадает с обычным сопряжением в алгебре кватернионов.

Если подалгебра $\mathscr{Q}$ не совпадает со всей алгеброй $\mathscr{A}$, то снова выберем единичный вектор e'', ортогональный $\mathscr{Q}$, и рассмотрим подалгебру $\mathscr{O} = \mathscr{Q} + \mathscr{Q}e''$, являющуюся удвоением $\mathscr{Q}$ и, следовательно, изоморфную алгебре октав (§ 6). Оказывается, эта подалгебра уже обязательно *совпадает с* $\mathscr{A}$, ибо, как мы докажем, любая подалгебра, содержащая **1** и *не совпадающая со всей алгеброй* $\mathscr{A}$, *ассоциативна*. Поскольку умножение октав не ассоциативно, подалгебра $\mathscr{O}$ обязана совпадать со всей алгеброй $\mathscr{A}$!

Подводя итог сказанному выше, мы получаем, что если алгебра $\mathscr{A}$ не изоморфна одной из алгебр $\mathscr{D}$, $\mathscr{K}$ или $\mathscr{Q}$, то она изоморфна алгебре $\mathscr{O}$. Но это и есть утверждение теоремы.

Итак, *теорема будет доказана, если мы проверим справедливость утверждений* I) *и* II), *а также докажем утверждение* III): *любая подалгебра* $\mathscr{U}$, *содержащая* **1** *и не совпадающая со всей алгеброй* $\mathscr{A}$, *ассоциативна*.

3°. **Две леммы.** Предварительно нам понадобятся две леммы. Мы рекомендуем читателю ознакомиться вначале с их формулировками, оставив доказательства для «второго чтения».

Лемма 1. *В любой нормированной алгебре* $\mathscr{A}$ *справедливо тождество*

$$(a_1 b_1, a_2 b_2) + (a_1 b_2, a_2 b_1) = 2(a_1, a_2)(b_1, b_2). \qquad (4)$$

Заметим, что это тождество связывает между собой четыре произвольных элемента a_1, a_2, b_1, b_2 алгебры $\mathcal{A}$.

Доказательство. Подставим в основное тождество (1) вместо элемента a сумму $a_1 + a_2$. Мы получим

$$(a_1b + a_2b,\ a_1b + a_2b) = (a_1 + a_2,\ a_1 + a_2)(b,\ b)$$

или

$$(a_1b,\ a_1b) + (a_2b,\ a_2b) + 2(a_1b,\ a_2b) = \\ = (a_1,\ a_1)(b,\ b) + (a_2,\ a_2)(b,\ b) + 2(a_1,\ a_2)(b,\ b).$$

Но в силу основного тождества первое и второе слагаемые левой части равны соответственно первому и второму слагаемым правой части. Следовательно,

$$(a_1b,\ a_2b) = (a_1,\ a_2)(b,\ b). \tag{5}$$

Чтобы получить требуемый результат, нужно в тождестве (5) заменить b на $b_1 + b_2$. Мы будем иметь тогда

$$(a_1b_1 + a_1b_2,\ a_2b_1 + a_2b_2) = (a_1,\ a_2)(b_1 + b_2,\ b_1 + b_2)$$

или

$$(a_1b_1,\ a_2b_1) + (a_1b_2,\ a_2b_2) + (a_1b_1,\ a_2b_2) + (a_1b_2,\ a_2b_1) = \\ = (a_1,\ a_2)(b_1,\ b_1) + (a_1,\ a_2)(b_2,\ b_2) + 2(a_1,\ a_2)(b_1,\ b_2).$$

Но в силу (5) первое и второе слагаемые левой части равны соответственно первому и второму слагаемым правой части. Вычеркивая равные слагаемые, приходим к тождеству (4).

Лемма 2. *В нормированной алгебре $\mathcal{A}$ с единицей справедливо тождество*

$$(ab)\overline{b} = (b,\ b)a. \tag{6}$$

Иначе говоря, элемент $(ab)\overline{b}$ всегда пропорционален a, причем коэффициент пропорциональности равен скалярному произведению (b, b).

Доказательство. Прежде всего заметим, что тождество (6) достаточно доказать для случая, когда $b \perp 1$. Действительно, пусть b' — произвольный элемент алгебры $\mathcal{A}$. Представим его в виде

$$b' = k1 + b,$$

где $b \perp 1$. Тогда $\overline{b} = -b$ и

$$(ab')\overline{b'} = (a(k1 + b))(k1 - b) = k^2a - (ab)b = k^2a + (ab)\overline{b}.$$

Если теперь предположить, что формула (6) справедлива для вектора b, то получим

$$(ab')\,\overline{b}' = k^2 a + (bb)\,a = [k^2 + (b, b)]\,a = (b', b')\,a\ ^*),$$

т. е. получим, что формула (6) справедлива для вектора b'.

Итак, будем доказывать тождество (6) в предположении, что $b \perp 1$ (или, что то же самое, $\overline{b} = -b$). Для сокращения дальнейших записей обозначим число (b, b) через λ.

Рассмотрим элемент

$$c = (ab)\,\overline{b} - \lambda a.$$

Мы должны показать, что $c = 0$ или, что то же самое,

$$(c, c) = 0.$$

В силу свойств скалярного произведения имеем

$$(c, c) = ((a, b)\,\overline{b}, (ab)\,\overline{b}) + \lambda^2 (a, a) - 2\lambda\,((ab)\,\overline{b}, a). \quad (7)$$

Правая часть состоит из трех слагаемых. Первое из них легко упрощается с помощью основного тождества (1):

$$((ab)\,\overline{b}, (ab)\,\overline{b}) = (ab, ab)\,(\overline{b}, \overline{b}) = (a, a)\,(b, b)^2 = \lambda^2 (a, a).$$

Для упрощения третьего слагаемого воспользуемся тождеством (4). Предварительно запишем это тождество в виде

$$(a_1 b_1, a_2 b_2) = 2\,(a_1, a_2)\,(b_1, b_2) - (a_1 b_2, a_2 b_1).$$

Полагая здесь

$$a_1 = ab, \quad b_1 = \overline{b}, \quad a_2 = a, \quad b_2 = 1,$$

будем иметь

$$((ab)\,\overline{b}, a) = 2\,(ab, a)\,(\overline{b}, 1) - (ab, \overline{ab}),$$

но первое слагаемое правой части равно нулю вследствие $b \perp 1$, а второе равно

$$-(ab, \overline{ab}) = (ab, ab) = (a, a)\,(b, b) = \lambda\,(a, a).$$

---

*) Из равенства $b' = k1 + b$ имеем $(b', b') = k^2 (1, 1) + (b, b)$; далее нужно учесть, что $(1, 1) = 1$, как легко следует из основного тождества (1) при $a = b = 1$.

Окончательно получаем

$$((ab)\bar{b}, a) = \lambda(a, a).$$

Возвращаясь к равенству (7), можем теперь записать

$$(c, c) = \lambda^2(a, a) + \lambda^2(a, a) - 2\lambda^2(a, a) = 0,$$

что и требовалось доказать.

Следствие леммы 2. Из тождества (6) мы выведем сейчас другое тождество, которое в дальнейших рассуждениях сыграет очень важную роль.

Подставим в (6) вместо b сумму $x + y$. Получим

$$(a(x + y))(\bar{x} + \bar{y}) = (x + y, x + y)a$$

или

$$(ax)\bar{x} + (ay)\bar{y} + (ax)\bar{y} + (ay)\bar{x} = \\ = (x, x)a + (y, y)a + 2(x, y)a.$$

Но в силу того же тождества (6) первое и второе слагаемые левой части равны соответственно первому и второму слагаемым правой части, следовательно,

$$(ax)\bar{y} + (ay)\bar{x} = 2(xy)a. \tag{8}$$

Это и есть требуемое тождество.

Из тождества (6) при $a = 1$ получается

$$b\bar{b} = (b, b)\,1.$$

Эта формула в сочетании с (6) дает

$$(ab)\bar{b} = a(b\bar{b});$$

отсюда тотчас следует

$$(ab)\,b = a(bb).$$

Аналогичными рассуждениями можно получить формулу

$$b(ba) = (bb)\,a.$$

Две последние формулы показывают, что алгебра $\mathcal{A}$ является альтернативной.

4°. Окончание доказательства теоремы. Мы приступаем теперь к доказательству утверждений I), II) и III). Напомним, что в этих утверждениях $\mathcal{U}$ обозначает любую подалгебру алгебры $\mathcal{A}$, содержащую 1 и не совпадающую со всей алгеброй, а e — любой вектор единичной длины, ортогональный $\mathcal{U}$.

Прежде всего установим, что *подпространства* $\mathcal{U}$ и $\mathcal{U}e$ *ортогональны друг другу*, т. е. что $u_1 \perp u_2 e$ для любых двух элементов $u_1 \in \mathcal{U}$, $u_2 \in \mathcal{U}$.

Для этого воспользуемся леммой 1. Если в тождестве (4) взять $a_1 = u_1$, $b_1 = u_2$, $a_2 = e$, $b_2 = 1$, то получим

$$(u_1 u_2, e) + (u_1, u_2 e) = 2(u_1, e)(u_2, 1).$$

Теперь нужно учесть, что $\mathcal{U}$ есть подалгебра и, значит, $u_1 u_2$ принадлежит $\mathcal{U}$. Итак, $u_1 \perp e$, $u_1 u_2 \perp e$; поэтому из написанного выше равенства следует

$$(u_1, u_2 e) = 0,$$

т. е. $u_1 \perp u_2 e$. Таким образом, подпространства $\mathcal{U}$ и $\mathcal{U}e$ ортогональны.

Отсюда легко следует утверждение I): *представление любого элемента из* $\mathcal{U} + \mathcal{U}e$ *в виде* $u_1 + u_2 e$ *возможно лишь единственным образом.* В самом деле, пусть

$$u_1 + u_2 e = u_1' + u_2' e.$$

Тогда

$$u_1 - u_1' = (u_2' - u_2) e$$

и, значит, элемент $v = u_1 - u_1'$ принадлежит одновременно подпространствам $\mathcal{U}$ и $\mathcal{U}e$. Но, по доказанному ранее, эти подпространства ортогональны друг другу; следовательно, $(v, v) = 0$ и тем самым $v = 0$. Это дает

$$u_1 - u_1' = 0 \quad \text{и} \quad (u_2' - u_2) e = 0.$$

Далее, легко видеть, что в силу основного тождества (1) из $ab = 0$ следует $a = 0$ или $b = 0$. В данном случае произведение $(u_2' - u_2) e$ равно 0, и поскольку $e \neq 0$, должно быть $u_2' - u_2 = 0$. Итак, $u_1 = u_1'$, $u_2 = u_2'$, и утверждение I) доказано.

Перейдем к доказательству утверждения II). Нам нужно проверить справедливость формулы (3). С этой целью докажем, что для любых двух элементов u и v из подалгебры $\mathcal{U}$ имеют место формулы

$$(ue)\, v = (u\bar{v})\, e, \qquad (\alpha)$$

$$u\,(ve) = (vu)\, e, \qquad (\beta)$$

$$(ue)\,(ve) = -\bar{v}u. \qquad (\gamma)$$

Из этих соотношений формула (3) вытекает очевидным образом. Действительно, по обычному правилу умноже-

ния суммы на сумму имеем

$$(u_1 + u_2 e)(v_1 + v_2 e) = u_1 v_1 + (u_2 e)(v_2 e) + (u_2 e) v_1 + u_1 (v_2 e)$$

и если последние три слагаемых правой части преобразовать по формулам (α), (β), (γ), то получим

$$(u_1 + u_2 e)(v_1 + v_2 e) = (u_1 v_1 - \bar{v}_2 u_2) + (v_2 u_1 + u_2 \bar{v}_1) e,$$

т. е. формулу (3).

Для доказательства (α), (β), (γ) будем исходить из доказанного ранее тождества (8):

$$(ax)\bar{y} + (ay)\bar{x} = 2(x, y)a. \tag{8}$$

Полагая в этом тождестве

$$a = u, \quad x = e, \quad y = \bar{v}$$

и учитывая, что $\bar{v} \perp e$, будем иметь

$$(ue)v + (u\bar{v})\bar{e} = 0.$$

Если учесть, что $\bar{e} = -e$ (ибо $e \perp 1$), то получаем формулу (α).

Чтобы доказать (β), положим в тождестве (8)

$$a = 1, \quad x = u, \quad y = \overline{ve}.$$

Учитывая, что $\overline{ve} = -ve$ (ибо $ve \perp \mathcal{U}$ и, значит, $ve \perp 1$), получим

$$u(ve) - (ve)\bar{u} = 0;$$

если теперь воспользоваться уже доказанной формулой (α), то будем иметь

$$u(ve) = (ve)\bar{u} = (vu)e.$$

Для вывода формулы (γ) воспользуемся следующим очевидным замечанием: если эта формула справедлива при $v = c$ и при $v = d$, то она справедлива и при $v = c + d$. Поскольку каждый элемент v можно представить в виде суммы двух слагаемых, из которых одно пропорционально 1, а другое ортогонально 1, то из сделанного выше замечания ясно, что формулу (γ) достаточно доказать для двух случаев: когда $v = k1$ и когда $v \perp 1$.

Если $v = k1$, то формула (γ) принимает вид

$$k(ue)e = -ku;$$

но такое равенство действительно имеет место в силу тождества (6).

Пусть $v \perp 1$ (и, следовательно, $\bar{v} = -v$). Полагая в тождестве (8)

$$a = u, \quad x = e, \quad y = -ve,$$

будем иметь

$$(ue)(ve) - (u(ve))\bar{e} = -2(e, ve)u.$$

Но выражение (e, ve) в силу тождества (5) равно $(1, v)(e, e)$, т. е. равно нулю. Далее, в силу (β) второе слагаемое левой части равно $-((vu)e)\bar{e} = -vu = \bar{v}u$. Отсюда

$$(ue)(ve) = -\bar{v}u,$$

что и требовалось получить. Итак, все три формулы (α), (β), (γ), а вместе с ними и утверждение II) доказаны.

Чтобы завершить доказательство теоремы, нам осталось сделать последний шаг: показать, что (утверждение III)) *любая подалгебра $\mathcal{U}$ алгебры $\mathcal{A}$, содержащая 1 и не совпадающая со всей алгеброй $\mathcal{A}$, ассоциативна*, т. е.

$$(uv)w = u(vw)$$

для любых трех элементов u, v, w из $\mathcal{U}$.

Для этой цели воспользуемся снова тождеством (8). Полагая в нем

$$a = ve, \quad x = \bar{w}, \quad y = \bar{u}e,$$

будем иметь

$$((ve)\bar{w})(-\bar{u}e) + ((ve)(\bar{u}e))w = 0$$

или, если применить формулы (α), (γ),

$$u(vw) - (uv)w = 0.$$

Доказательство теоремы Гурвица теперь полностью завершено.

§ 18. Способ построения любой нормированной алгебры и вытекающие из него следствия для задачи о сумме квадратов

1°. Способ построения новых нормированных алгебр. Прежде всего укажем один специальный прием, с помощью которого можно, исходя из данной нормированной алгебры $\mathcal{A}$, построить много других нормированных алгебр.

Пусть A и B — два ортогональных преобразования в $\mathscr{A}$ (т. е. два преобразования, сохраняющих норму любого элемента $x \in \mathscr{A}$). Определим в векторном пространстве алгебры $\mathscr{A}$ новое умножение — будем обозначать его с помощью значка «$\circ$» — по формуле

$$u \circ v = A(u)\, B(v). \tag{1}$$

Как видно из этого определения, для того, чтобы получить произведение элементов u и v в новом смысле, следует взять вместо u и v элементы $A(u)$ и $B(v)$ и перемножить их в старом смысле.

Нетрудно убедиться, что для новой операции справедливы такие соотношения:

$$u \circ (v_1 + v_2) = u \circ v_1 + u \circ v_2, \quad u \circ kv = k(u \circ v)$$

и

$$(u_1 + u_2) \circ v = u_1 \circ v + u_2 \circ v, \quad ku \circ v = k(u \circ v);$$

первые два из написанных равенств вытекают из линейности преобразования B, два других — из линейности A. Эти соотношения показывают, что новая операция «$\circ$» действительно является умножением (см. 7° § 7).

Векторное пространство алгебры $\mathscr{A}$, снабженное новой операцией умножения, обозначим $\mathscr{A}_0$. Таким образом, $\mathscr{A}$ и $\mathscr{A}_0$ — это одно и то же векторное пространство, но снабженное различными операциями умножения.

В алгебре $\mathscr{A}$ по условию задано скалярное произведение (x, y). Оказывается, что по отношению к этому скалярному произведению новая алгебра $\mathscr{A}_0$, подобно старой, будет также нормированной.

В самом деле, из формулы (1) следует

$$|u \circ v| = |A(u)\, B(v)| = |A(u)|\,|B(v)| = |u|\,|v|;$$

здесь мы воспользовались нормированностью исходной алгебры $\mathscr{A}$, а также тем, что преобразования A и B — ортогональные, т. е.

$$|A(u)| = |u| \quad \text{и} \quad |B(v)| = |v|.$$

2°. Конструкция произвольной нормированной алгебры. Указанным выше способом можно из одной нормированной алгебры $\mathscr{A}$ получать много других; для этого в формулу (1) нужно подставлять те или иные ортогональные преобразования A и B. Нам известны четыре

замечательных нормированных алгебры: действительных чисел, комплексных чисел, кватернионов, октав. Нельзя ли, применяя к ним описанную методику, получить все вообще нормированные алгебры? Оказывается, что можно. Поскольку по теореме Гурвица указанными четырьмя алгебрами исчерпываются все нормированные алгебры с единицей, то нам нужно доказать следующую теорему.

Теорема. *Любая нормированная алгебра* $\mathcal{A}_0$ *может быть получена из некоторой нормированной алгебры* $\mathcal{A}$ *с единицей введением нового умножения по формуле* (1) (в этой формуле $\circ$ обозначает умножение в алгебре $\mathcal{A}_0$).

Для доказательства возьмем любой элемент $e \in \mathcal{A}_0$ с нормой, равной 1, и рассмотрим преобразование алгебры $\mathcal{A}_0$, при котором каждый ее элемент x переходит в $x \circ e$. Такого рода преобразование (умножение справа на e) называется *правым сдвигом на элемент* e в алгебре $\mathcal{A}_0$; обозначим его кратко A. Итак, мы вводим преобразование

$$A(x) = x \circ e.$$

Нетрудно видеть, что преобразование A — ортогональное. Действительно, из равенств

$$|A(x)| = |x \circ e| = |x||e| = |x|$$

следует, что преобразование A сохраняет норму любого элемента x.

Аналогичным образом можно рассмотреть другое преобразование

$$B(x) = e \circ x$$

— *левый сдвиг на элемент* e в алгебре $\mathcal{A}_0$ — и показать, что оно также является ортогональным.

Из ортогональности преобразований A и B вытекает (§ 13) существование обратных преобразований A^{-1} и B^{-1}, а также их ортогональность *).

*) Сделаем одно попутное замечание. Существование преобразований A^{-1} и B^{-1} означает, что каждое из уравнений

$$x \circ e = a \quad \text{и} \quad e \circ y = a$$

имеет решение, и притом единственное. Тот факт, что $|e| = 1$, здесь, конечно, роли не играет; важно только, что $e \neq 0$. Отсюда можно сделать такое заключение: *любая нормированная алгебра есть алгебра с делением.*

Используя эти преобразования, мы введем сейчас в векторном пространстве алгебры $\mathscr{A}_0$ новый закон умножения. А именно, произведение элементов x и y в новом смысле определим формулой

$$xy = A^{-1}(x) \circ B^{-1}(y). \tag{2}$$

Полученную таким образом новую алгебру обозначим $\mathscr{A}$.

Написанное равенство выражает новое умножение через старое. Но из него легко получить и выражение старого умножения через новое: полагая

$$A^{-1}(x) = u, \quad B^{-1}(y) = v,$$

будем иметь

$$A(u)\,B(v) = u \circ v.$$

Таким образом, если принять алгебру $\mathscr{A}$ с операцией умножения uv за исходную, то данная нам с самого начала алгебра $\mathscr{A}_0$ будет получаться из нее заменой умножения новым умножением $u \circ v$ по формуле

$$u \circ v = A(u)\,B(v).$$

Чтобы завершить доказательство теоремы, теперь остается только показать, что алгебра $\mathscr{A}$ обладает единицей.

Проверим, что роль единицы в алгебре $\mathscr{A}$ играет элемент $\tilde{e} = e \circ e$. В самом деле, рассмотрим два произведения,

$$x\tilde{e} \quad \text{и} \quad \tilde{e}y.$$

Для первого из них имеем –

$$x\tilde{e} = A^{-1}(x) \circ B^{-1}(\tilde{e}).$$

По определению обратного преобразования, элемент $u = B^{-1}(\tilde{e})$ является (единственным) решением уравнения

$$B(u) = \tilde{e}$$

или, что то же, уравнения $e \circ u = e \circ e$; отсюда ясно (в силу единственности), что этот элемент равен e. Далее, $v = A^{-1}(x)$ означает, что $x = A(v)$, т. е. $v \circ e = x$.

Учитывая это, получим

$$x\tilde{e} = A^{-1}(x) \circ B^{-1}(\tilde{e}) = v \circ e = x.$$

Точно так же находим, что

$$\tilde{e}y = A^{-1}(\tilde{e}) \circ B^{-1}(y) = e \circ B^{-1}(y) = y.$$

Этим мы показали, что $\tilde{e}$ — единица алгебры $\mathscr{A}$. Теорема доказана полностью.

Итак, все *без исключения нормированные алгебры могут быть получены из четырех известных алгебр* $\mathscr{D}$, $\mathscr{K}$, $\mathscr{Q}$, $\mathscr{O}$ *введением нового умножения по формуле* (1). До известной степени этот факт можно рассматривать как способ описания всех нормированных алгебр.

3°. Число n в тождестве (!). В качестве одного из следствий теоремы мы получаем, что размерность любой нормированной алгебры равна одному из чисел 1, 2, 4, 8 (размерности алгебр действительных чисел, комплексных чисел, кватернионов и октав соответственно).

Вспомним теперь, что существует определенная связь между нормированными алгебрами и тождествами вида

$$(x_1^2 + x_2^2 + \ldots + x_n^2)(y_1^2 + y_2^2 + \ldots + y_n^2) = \\ = \Phi_1^2 + \Phi_2^2 + \ldots + \Phi_n^2. \quad (!)$$

Это связь (см. § 17) заключается в том, что, взяв любую нормированную алгебру размерности n, выбрав в ней произвольный ортонормированный базис и записав закон умножения в этом базисе, получим n форм $\Phi_1, \Phi_2, \ldots, \Phi_n$, удовлетворяющих тождеству (!); более того, таким путем могут быть получены все без исключения тождества (!). Учитывая эту связь, мы делаем следующее фундаментальное заключение.

Число n в тождестве (!) *может быть равно только одному из четырех чисел*: 1, 2, 4 *и* 8.

4°. Обозрение всех тождеств (!). Конечно, из доказанной выше теоремы можно вывести нечто большее, нежели только заключение о числе квадратов в тождестве (!). В самом деле, зная способ построения любой нормированной алгебры, мы тем самым имеем некоторый способ дать описание всех тождеств (!). Покажем, что все такие тождества получаются следующим путем.

Для данного n, равного одному из чисел 2, 4 *или* 8, *нужно в соответствующей алгебре* $\mathscr{K}$, $\mathscr{Q}$ *или* $\mathscr{O}$ *взять три ортонормированных базиса*

$$e_1, e_2, \ldots, e_n; \quad k_1, k_2, \ldots, k_n; \quad i_1, i_2, \ldots, i_n,$$

разложить произвольный вектор x по первому базису, произвольный вектор y — по второму, а их произведение — по третьему, т. е. записать

$$x = \sum_{\alpha} x_\alpha e_\alpha, \quad y = \sum_{\beta} y_\beta k_\beta, \quad xy = \sum_{\gamma} \Phi_\gamma i_\gamma.$$

Тогда набор форм $\Phi_\gamma(x_1, \ldots, x_n; y_1, \ldots, y_n)$ *) удовлетворяет тождеству* (!), *причем таким путем может быть получено любое тождество* (!).

Что указанный путь всегда приводит к формам, удовлетворяющим (!), следует из равенства

$$\left(\sum_{\alpha} x_\alpha e_\alpha\right)\left(\sum_{\beta} y_\beta k_\beta\right) = \sum_{\gamma} \Phi_\gamma i_\gamma.$$

Действительно, беря норму от обеих частей равенства, получаем тождество (!).

Обратно, покажем, что любое тождество (!) может быть получено указанным образом. Мы уже знаем, что любое тождество (!) получается, если рассмотреть закон умножения вида

$$x \circ y = A(x)\, B(y)$$

(где A и B — ортогональные преобразования) и записать его в произвольном ортонормированном базисе $i_1, i_2, \ldots, i_n$. Другими словами, формы $\Phi_1, \Phi_2, \ldots, \Phi_n$, входящие в данное тождество, берутся из равенства

$$A\left(\sum_{\alpha} x_\alpha i_\alpha\right)\, B\left(\sum_{\beta} y_\beta i_\beta\right) = \sum_{\gamma} \Phi_\gamma i_\gamma. \tag{3}$$

Но в силу линейности преобразований A и B имеем

$$A\left(\sum_{\alpha} x_\alpha i_\alpha\right) = \sum_{\alpha} x_\alpha A(i_\alpha), \quad B\left(\sum_{\beta} y_\beta i_\beta\right) = \sum_{\beta} y_\beta B(i_\beta).$$

Обозначая $A(i_\alpha)$ через e_α, а $B(i_\beta)$ через k_β, придем к следующей записи равенства (3):

$$\left(\sum_{\alpha} x_\alpha e_\alpha\right)\left(\sum_{\beta} y_\beta k_\beta\right) = \sum_{\gamma} \Phi_\gamma i_\gamma.$$

Учитывая теперь, что каждый из наборов $e_1, e_2, \ldots, e_n$ и $k_1, k_2, \ldots, k_n$ является ортонормированным базисом, приходим к заключению, что набор форм $\Phi_1, \Phi_2, \ldots, \Phi_n$ получается так, как указано выше.

---

*) Чтобы фактически найти выражения для форм Φ_γ, нужно записать

$$xy = \left(\sum_{\alpha} x_\alpha e_\alpha\right)\left(\sum_{\beta} y_\beta k_\beta\right) = \sum_{\alpha,\,\beta} x_\alpha y_\beta e_\alpha k_\beta$$

и каждое произведение $e_\alpha k_\beta$ заменить его разложением по $i_1, i_2, \ldots, i_n$.

Для более подготовленного читателя приведем то же самое обозрение тождеств (!) в других терминах. При данном $n = 1, 2, 4, 8$ нужно взять какой-либо один определенный набор $\Phi_1, \Phi_2, \ldots, \Phi_n$ и менять его следующим образом: переменные $x_1, x_2, \ldots, x_n$ в выражении для Φ_i заменяются переменными $x_1', x_2', \ldots, x_n'$, выражающимися через $x_1, x_2, \ldots, x_n$ с помощью некоторого ортогонального преобразования A; аналогичная операция производится над $y_1, y_2, \ldots, y_n$ с помощью другого ортогонального преобразования B. После этого получившийся набор форм $\Phi_1', \Phi_2', \ldots, \Phi_n'$ подвергается третьему ортогональному преобразованию C.

Условимся считать два тождества (!) *эквивалентными*, если одно из них получается из другого только что указанным способом. Тогда будет справедливо следующее предложение: *при данном* $n = 1, 2, 4, 8$ *существует только одно, с точностью до эквивалентности, тождество* (!).

5°. Примеры нормированных алгебр размерностей 2 и 4 и связанных с ними тождеств (!). Среди нормированных алгебр размерности 2 только одна, как мы знаем, обладает единицей; это — алгебра $\mathcal{K}$ комплексных чисел. Учитывая, что переход к сопряженному комплексному числу:

$$x \to \bar{x}$$

есть ортогональное преобразование алгебры $\mathcal{K}$ (ибо $|\bar{x}| = |x|$), мы можем построить еще по крайней мере три новых алгебры. Для этого обычное умножение xy комплексных чисел заменяем новыми операциями

$$\begin{aligned} x \textcircled{1} y &= \bar{x}y, \\ x \textcircled{2} y &= x\bar{y}, \\ x \textcircled{3} y &= \bar{x}\bar{y}. \end{aligned} \tag{4}$$

Получаются три новых нормированных алгебры $\mathcal{K}_1$, $\mathcal{K}_2$, $\mathcal{K}_3$.

В качестве полезного упражнения предлагаем читателю доказать, что любая нормированная алгебра размерности 2 изоморфна одной из алгебр $\mathcal{K}$, $\mathcal{K}_1$, $\mathcal{K}_2$, $\mathcal{K}_3$, причем среди этих четырех алгебр никакие две не изоморфны.

Приведем теперь примеры тождеств (!), связанных с только что описанными алгебрами.

Для алгебры $\mathcal{K}_1$ в базисе $1, i$ имеем

$$\begin{aligned} x \textcircled{1} y = \bar{x}y = (x_1 - x_2 i)(y_1 + y_2 i) = \\ = (x_1 y_1 + x_2 y_2) + (x_1 y_2 - x_2 y_1) i, \end{aligned}$$

поэтому соответствующее тождество будет

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2.$$

Оно, как видим, несколько отличается от уже знакомого нам тождества

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2, \quad (5)$$

отвечающего в том же базисе $1, i$ алгебре $\mathcal{K}$.

Тождество, более отличающееся от (5), можно получить, приняв в качестве исходной алгебру $\mathcal{K}$, и выбрав в ней за базисные векторы элементы

$$e_1 = \frac{1}{\sqrt{2}}(1 + i) \quad \text{и} \quad e_2 = \frac{1}{\sqrt{2}}(1 - i).$$

Нетрудно проверить, что эти два элемента образуют ортонормированный базис. Запишем в этом базисе закон умножения:

$$(u_1e_1 + u_2e_2)(v_1e_1 + v_2e_2) =$$
$$= \frac{1}{\sqrt{2}}(u_1v_2 + v_1u_2 + u_1v_1 - u_2v_2)\,e_1 +$$
$$+ \frac{1}{\sqrt{2}}(u_1v_2 + v_1u_2 - u_1v_1 + u_2v_2)\,e_2.$$

Соответствующее тождество будет

$$(u_1^2 + u_2^2)(v_1^2 + v_2^2) = \left[\frac{1}{\sqrt{2}}(u_1v_2 + v_1u_2 + u_1v_1 - u_2v_2)\right]^2 +$$
$$+ \left[\frac{1}{\sqrt{2}}(u_1v_2 + v_1u_2 - u_1v_1 + u_2v_2)\right]^2.$$

Обратимся к нормированным алгебрам размерности 4. В этом случае единственная алгебра с единицей — это, как мы знаем, алгебра $\mathcal{Q}$ кватернионов. Так же, как в случае комплексных чисел, операция сопряжения есть ортогональное преобразование алгебры $\mathcal{Q}$. Поэтому существует еще по крайней мере три нормированных алгебры размерности 4 — $\mathcal{Q}_1$, $\mathcal{Q}_2$, $\mathcal{Q}_3$ с умножением, определенным по формулам (4). Однако в четырехмерном случае существуют еще и другие нормированные

алгебры, например, алгебры с умножениями вида

$$axyb,$$

$$\bar{a}xyb,$$

$$ax\bar{y}b,$$

$$\bar{a}x\bar{y}b,$$

где a и b — два фиксированных кватерниона.

Можно показать (предоставляем это читателю), что любая нормированная алгебра размерности 4 изоморфна одной из алгебр такого вида.

Рассмотрим в качестве примера первое из указанных умножений при $a = i$, $b = j$. Мы получаем нормированную алгебру $\tilde{Q}$ с законом умножения

$$x \circ y = (ix)(yj).$$

Найдем, какое тождество (!) отвечает этой алгебре, если в качестве базисных элементов взять 1, i, j, k.

Имеем

$$x \circ y = (i(x_0 + x_1 i + x_2 j + x_3 k))((y_0 + y_1 i + y_2 j + y_3 k) j) =$$
$$= (x_0 i - x_1 + x_2 k - x_3 j)(y_0 j + y_1 k - y_2 - y_3 i) =$$
$$= (x_1 y_2 - x_2 y_1 + x_0 y_3 + x_3 y_0) + (-x_0 y_2 - x_2 y_0 + x_1 y_3 - x_3 y_1) i +$$
$$+ (-x_1 y_0 - x_0 y_1 + x_3 y_2 - x_2 y_1) j + (x_0 y_0 - x_1 y_1 - x_2 y_2 - x_3 y_3) k.$$

Соответствующее тождество будет

$$(x_0^2 + x_1^2 + x_2^2 + x_3^2)(y_0^2 + y_1^2 + y_2^2 + y_3^2) =$$
$$= (x_1 y_2 - x_2 y_1 + x_0 y_3 + x_3 y_0)^2 + (-x_0 y_2 - x_2 y_0 + x_1 y_3 - x_3 y_1)^2 +$$
$$+ (-x_1 y_0 - x_0 y_1 + x_3 y_2 - x_2 y_1)^2 + (x_0 y_0 - x_1 y_1 - x_2 y_2 - x_3 y_3)^2.$$

Примеров тождества (!) для $n = 8$ (отличных от «стандартного» тождества на стр. 44) мы здесь не приводим, так как они громоздки, а получение их принципиальных трудностей не представляет.

§ 19. Теорема Фробениуса

1°. Формулировка теоремы Фробениуса. Одна из классических задач теории алгебр — это разыскание всех алгебр с делением. Несмотря на ее, казалось бы, фундаментальный характер (а также несмотря на то, что в решение этой задачи упирается ряд вопросов из

других разделов математики, например, топологии), эта задача в полном объеме не решена до сих пор. Важный результат был получен совсем недавно. Он состоит в том, что размерность любой из таких алгебр равна одному из чисел 1, 2, 4, 8. Хотя, как видно отсюда, размерности алгебр с делением не слишком велики, все же полного обозрения этих алгебр нет и сейчас.

Однако, если помимо существования деления, мы наложим на искомую алгебру еще и другие требования естественного характера, то, разумеется, наша задача станет значительно легче. В 1878 г. немецкий математик Г. Фробениус доказал следующую замечательную теорему.

Теорема Фробениуса. *Любая ассоциативная алгебра с делением изоморфна одной из трех: алгебре действительных чисел, алгебре комплексных чисел или алгебре кватернионов.*

Впоследствии был установлен более общий результат, который можно назвать обобщенной теоремой Фробениуса.

Обобщенная теорема Фробениуса. *Любая альтернативная алгебра с делением изоморфна одной из четырех алгебр: действительных чисел, комплексных чисел, кватернионов или октав.*

Напомним, что альтернативной называется такая алгебра, в которой для любых двух элементов a и b справедливы равенства

$$(ab)b = a(bb)$$

и

$$(bb)a = b(ba).$$

Очевидно, что любая ассоциативная алгебра автоматически является альтернативной, поэтому теорема Фробениуса вытекает из обобщенной теоремы Фробениуса (следует учесть, что алгебра октав не ассоциативна).

Чтобы доказать обе сформулированные выше теоремы, мы перечислим сначала некоторые свойства ассоциативной алгебры с делением. Затем будет показано, как из этих свойств выводится теорема Фробениуса. Доказательства самих свойств будут даны вслед за этим. В последнем пункте параграфа будет приведено доказательство обобщенной теоремы Фробениуса, использующее теорему Гурвица.

2° **Три утверждения о свойствах ассоциативной алгебры с делением.**

Утверждение I. *Алгебра* $\mathcal{A}$ *содержит единицу.*

Утверждение II. *Если элемент* $a \in \mathcal{A}$ *не пропорционален* 1, *то совокупность* $\mathcal{K}_a$ *элементов вида*

$$\alpha 1 + \beta a$$

образует подалгебру, изоморфную алгебре комплексных чисел.

Утверждение III. *Если элементы* $a_1 \in \mathcal{A}$, $a_2 \in \mathcal{A}$ *не принадлежат одной подалгебре* $\mathcal{K}_a$, *то совокупность* Q_{a_1, a_2} *элементов вида*

$$\alpha 1 + \beta a_1 + \gamma a_2 + \delta a_1 a_2$$

образует подалгебру, изоморфную алгебре кватернионов.

Отметим, что в процессе доказательства утверждения III будет установлен следующий факт: *если* b_1 *и* b_2 *— два элемента, квадраты которых равны* -1, *то*

$$b_1 b_2 + b_2 b_1 = \lambda 1, \qquad (1)$$

где λ *— действительное число.*

3°. **Доказательство теоремы Фробениуса.** Исходя из утверждений I, II, III, уже совсем нетрудно доказать теорему Фробениуса. Пусть $\mathcal{A}$ — ассоциативная алгебра с делением. Согласно утверждению I, алгебра $\mathcal{A}$ обладает единицей. Элементы вида $k1$ образуют подалгебру $\mathcal{D}$, изоморфную алгебре действительных чисел. Если $\mathcal{D}$ не совпадает со всей алгеброй $\mathcal{A}$, то, согласно утверждению II, в $\mathcal{A}$ содержится подалгебра $\mathcal{K}_a$, изоморфная алгебре комплексных чисел. Если $\mathcal{K}_a$ не совпадает со всей алгеброй $\mathcal{A}$, то, согласно утверждению III, в $\mathcal{A}$ содержится подалгебра $Q_{a,b}$, изоморфная алгебре кватернионов. В случае, когда $Q_{a,b}$ совпадает со всей алгеброй $\mathcal{A}$, доказывать больше нечего. Предположим поэтому, что существует элемент c, не принадлежащий $Q_{a,b}$, и покажем, что тогда A не может быть алгеброй с делением.

В кватернионной алгебре $Q_{a,b}$ выберем базис 1, i, j, k со «стандартной» таблицей умножения:

$$i^2 = j^2 = k^2 = -1,$$

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j,$$

а элемент c представим в виде $p\mathbf{1} + qe$, где $e^2 = -\mathbf{1}$ (e есть «мнимая единица» комплексной алгебры $\mathscr{K}_c$).

Преобразуем теперь элемент ie, используя ассоциативность умножения в алгебре $\mathscr{A}$, а также соотношение (1). Имеем

$$ie = (jk)e = j(ke) = j(-ek + \lambda'\mathbf{1}) = -(je)k + \lambda' j =$$
$$= -(-ej + \lambda''\mathbf{1})k + \lambda' j = ei - \lambda'' k + \lambda' j$$

и, следовательно,

$$ie - ei = \lambda' j - \lambda'' k.$$

С другой стороны, опять в силу (1),

$$ie + ei = \lambda'''\mathbf{1}.$$

Складывая эти два равенства, находим, что ie есть элемент из $\mathscr{Q}_{a,b}$. Следовательно, $ic = i(p\mathbf{1} + qe)$ есть также элемент из $\mathscr{Q}_{a,b}$. Мы видим, что умножение i на любой элемент, не принадлежащий $\mathscr{Q}_{a,b}$, дает элемент из $\mathscr{Q}_{a,b}$. Но и в том случае, когда $c' \in \mathscr{Q}_{a,b}$, произведение ic' есть элемент из $\mathscr{Q}_{a,b}$. Таким образом, элемент i в произведении с любым элементом алгебры $\mathscr{A}$ дает элемент из $\mathscr{Q}_{a,b}$. Но это невозможно, если $\mathscr{A}$ есть алгебра с делением (уравнение $ix = c$, где c не содержится в $\mathscr{Q}_{a,b}$, оказывается неразрешимым). Этим (если считать справедливыми утверждения I, II, III) доказана теорема Фробениуса.

4°. Доказательство утверждений I, II, III. Итак, чтобы завершить доказательство теоремы Фробениуса, нам осталось только проверить справедливость утверждений I, II и III.

Доказательство утверждения I. Пусть a — какой-нибудь отличный от нуля элемент алгебры $\mathscr{A}$. Рассмотрим уравнение

$$xa = a.$$

Так как $\mathscr{A}$ есть алгебра с делением, то написанное уравнение имеет решение, и притом единственное; обозначим это решение (т. е. искомый элемент x) через e. Итак, $ea = a$. Умножая обе части этого равенства слева на b, получим $b(ea) = ba$, или, учитывая ассоциативность алгебры $\mathscr{A}$, $(be)a = ba$. Ввиду единственности решения уравнения $xa = ba$, отсюда следует

$$be = b.$$

Умножая теперь полученное соотношение справа на c и рассуждая аналогично, находим

$$ec = c.$$

Поскольку элементы b и c произвольны, то два последних равенства означают, что элемент e является единицей алгебры $\mathcal{A}$. В дальнейшем единицу алгебры будем обозначать, как обычно, 1.

Доказательство утверждения II. Для нашей цели достаточно показать, что элемент a удовлетворяет квадратному уравнению

$$a^2 + sa + t1 = 0 \tag{2}$$

с отрицательным дискриминантом *).

Рассмотрим последовательные степени элемента a:

$$a^0 = 1,\ a^1,\ a^2,\ a^3,\ \ldots,\ a^n,$$

где n — размерность алгебры. Из теоремы 2 § 9 вытекает, что эта система из $n+1$ векторов линейно зависима, т. е. что некоторая степень должна разлагаться по предыдущим:

$$a^m = k_{m-1}a^{m-1} + \ldots + k_2a^2 + k_1a + k_0 1.$$

Иначе говоря, элемент a удовлетворяет уравнению m-й степени

$$x^m - k_{m-1}x^{m-1} - \ldots - k_2x^2 - k_1x - k_0 1 = 0.$$

Выражению, стоящему в левой части этого уравнения, можно сопоставить обычный многочлен m-й степени

$$x^m - k_{m-1}x^{m-1} - \ldots - k_2x^2 - k_1x - k_0;$$

обозначим его коротко $P(x)$.

Как известно, любой многочлен с действительными коэффициентами может быть разложен в произведение многочленов первой и второй степеней; при этом, разумеется, можно считать, что каждый множитель второй

*) Действительно, из (2) следует $a^2 = -sa - t1$, значит, множество элементов вида $\alpha 1 + \beta a$ замкнуто относительно умножения; тем самым указанное множество является гиперкомплексной системой размерности 2. Согласно 2° § 2, при $\frac{s^2}{4} - t < 0$ (отрицательность дискриминанта) такая система изоморфна системе комплексных чисел.

степени уже неразложим (в произведение двух множителей первой степени). Итак,

$$P(x) = P_1(x)\,P_2(x)\,\ldots\,P_s(x), \tag{3}$$

где каждый из множителей правой части есть либо многочлен первой степени, либо неразложимый многочлен второй степени.

Чтобы понять дальнейшее рассуждение, читатель должен отчетливо представлять смысл равенства (3). Каждый из многочленов $P_1(x), \ldots, P_s(x)$ представляет собой сумму двух или трех членов:

$$x + t \quad \text{или} \quad x^2 + sx + t.$$

Равенство (3) говорит о том, что если перемножить выражения $P_1(x), \ldots, P_s(x)$ по правилу умножения суммы на сумму, затем воспользоваться формулой

$$x^k \cdot x^l = x^{k+l}$$

и сделать приведение подобных членов, то получится выражение $P(x)$.

Но правила действий над степенями элемента a — те же, что и над степенями неизвестной x:

$$a^k \cdot a^l = a^{k+l}$$

(ведь алгебра $\mathscr{A}$ предполагается ассоциативной). Отсюда видно, что равенство (3) останется в силе, если вместо неизвестной x подставить элемент a:

$$P(a) = P_1(a)\,P_2(a)\,\ldots\,P_s(a).$$

Но поскольку $P(a) = 0$, то

$$P_1(a)\,P_2(a)\,\ldots\,P_s(a) = 0. \tag{4}$$

Воспользуемся далее тем, что $\mathscr{A}$ есть алгебра с делением. Из этого факта вытекает, что если произведение нескольких элементов равно нулю, то хотя бы один из множителей равен 0 (действительно, если $uv = 0$ и $u \neq 0$, то ввиду единственности решения уравнения $ux = 0$ должно быть $v = 0$). В применении к (4) это означает, что для некоторого номера i

$$P_i(a) = 0,$$

т. е. что элемент a удовлетворяет уравнению первой или второй степени. Однако уравнение первой степени получиться для a не может, ибо тогда

$$a + t1 = 0,$$

т. е. элемент a пропорционален 1, вопреки условию леммы. Следовательно, a удовлетворяет некоторому квадратному уравнению (2). Так как при этом многочлен второй степени $P_i(x)$ неразложим, то его дискриминант должен быть отрицательным числом. Утверждение II доказано.

Доказательство утверждения III. Выберем в подалгебре $\mathcal{K}_{a_1}$ такой элемент b_1, что $b_1^2 = -1$ (b_1 есть «мнимая единица» в комплексной алгебре $\mathcal{K}_{a_1}$). Аналогичным образом в подалгебре $\mathcal{K}_{a_2}$ выберем элемент b_2 такой, что $b_2^2 = -1$. Так как b_1, b_2 отличаются от a_1, a_2 (соответственно) на слагаемые, кратные 1, то совокупность элементов вида $\alpha 1 + \beta a_1 + \gamma a_2 + \delta a_1 a_2$ совпадает с совокупностью элементов вида $\alpha' 1 + \beta' b_1 + \gamma' b_2 + \delta' b_1 b_2$, иначе говоря, $\mathcal{Q}_{a_1, a_2}$ совпадает с $\mathcal{Q}_{b_1, b_2}$.

Далее, нетрудно видеть, что если

$$e_1 = b_1, \quad e_2 = k_1 b_1 + k_2 b_2,$$

причем $k_2 \neq 0$, то множество $\mathcal{Q}_{e_1, e_2}$ будет то же самое, что $\mathcal{Q}_{b_1, b_2}$, а значит, и $\mathcal{Q}_{a_1, a_2}$. *Покажем, что числа* k_1 *и* k_2 *можно выбрать так, чтобы были справедливы равенства*

$$e_1^2 = -1, \quad e_2^2 = -1, \quad (e_1 e_2)^2 = -1 \tag{5}$$

(впрочем, первое равенство справедливо при любом выборе k_1, k_2).

Для этой цели запишем, что

$$(b_1 + b_2)^2 = b_1^2 + b_2^2 + (b_1 b_2 + b_2 b_1) = -2 \cdot 1 + (b_1 b_2 + b_2 b_1),$$

но, с другой стороны, квадрат элемента $b_1 + b_2$ должен разлагаться по 1 и $b_1 + b_2$:

$$(b_1 + b_2)^2 = p1 + q(b_1 + b_2).$$

Следовательно,

$$b_1 b_2 + b_2 b_1 = (p + 2) 1 + q(b_1 + b_2). \tag{6}$$

Аналогично,

$$(b_1 + 2b_2)^2 = b_1^2 + 4b_2^2 + 2(b_1b_2 + b_2b_1) = \\ = -5 \cdot 1 + 2(b_1b_2 + b_2b_1)$$

и

$$(b_1 + 2b_2)^2 = p'1 + q'(b_1 + 2b_2);$$

следовательно,

$$b_1b_2 + b_2b_1 = \frac{1}{2}(p' + 5)1 + \frac{1}{2}q'(b_1 + 2b_2).$$

Если бы было $q \neq 0$, то, приравняв два выражения для $b_1b_2 + b_2b_1$, мы получили бы, что b_1 отличается от b_2 на элемент, кратный 1, т. е. $b_2 \in \mathcal{K}_{b_1}$, что исключено условием. Следовательно, $q = 0$ и равенство (6) дает

$$b_1b_2 + b_2b_1 = \lambda 1. \qquad (1)$$

Итак, *если* b_1, b_2 *— два элемента, квадраты которых равны* -1, *то справедливо равенство* (1).

Теперь нетрудно определить искомые элементы e_1 и e_2. Рассмотрим для этой цели элемент $c = \lambda b_1 + 2b_2$, где λ взято из равенства (1). Его квадрат равен

$$c^2 = -\lambda^2 1 - 4 \cdot 1 + 2\lambda(b_1b_2 + b_2b_1) = (\lambda^2 - 4) \cdot 1, \qquad (7)$$

поэтому должно быть $\lambda^2 - 4 < 0$ *). Положим

$$e_2 = \frac{1}{\sqrt{4 - \lambda^2}}\, c,$$

тогда из (7) будет следовать, что $e_2^2 = -1$, т. е. второе из равенств (5). Чтобы установить третье, заметим сначала, что

$$e_1e_2 + e_2e_1 = 0; \qquad (8)$$

это следует из

$$e_1e_2 + e_2e_1 = \frac{1}{\sqrt{4 - \lambda^2}}(b_1(\lambda b_1 + 2b_2) + (\lambda b_1 + 2b_2)b_1) = \\ = \frac{1}{\sqrt{4 - \lambda^2}}(-2\lambda \cdot 1 + 2(b_1b_2 + b_2b_1)) = 0.$$

*) Если бы было $\rho = \lambda^2 - 4 \geqslant 0$, то из $c^2 = \rho 1$ следовало бы $(c - \sqrt{\rho} \cdot 1)(c + \sqrt{\rho} \cdot 1) = 0$, т. е. $c = \sqrt{\rho} \cdot 1$ или $c = -\sqrt{\rho} \cdot 1$. Но это невозможно, так как b_1 и b_2 не лежат в одной комплексной подалгебре.

Используя (8), получаем

$$(e_1e_2)^2 = (e_1e_2)(e_1e_2) = (e_1e_2)(-e_2e_1) = \\ = -(e_1e_2^2)e_1 = e_1^2 = -1, \quad (9)$$

что и завершает доказательство равенств (5).

Установим теперь, что множество $\mathcal{Q}_{e_1, e_2}$ элементов вида

$$\alpha 1 + \beta e_1 + \gamma e_2 + \delta e_1e_2$$

(совпадающее, как уже говорилось, с $\mathcal{Q}_{a_1, a_2}$) есть подалгебра алгебры $\mathcal{A}$.

Для этого достаточно проверить, что произведение любых двух элементов из четверки

$$1, \ e_1, \ e_2, \ e_1e_2 \quad (10)$$

разлагается по тем же четырем элементам. Нам уже известны все произведения, кроме следующих:

$$e_1(e_1e_2), \quad (e_1e_2)e_1, \quad e_2(e_1e_2), \quad (e_1e_2)e_2.$$

Каждое из них легко вычисляется:

$$\begin{aligned} &e_1(e_1e_2) = e_1^2e_2 = -e_2, \\ &(e_1e_2)e_1 = -(e_2e_1)e_1 = -e_2e_1^2 = e_2, \\ &e_2(e_1e_2) = -e_2(e_2e_1) = -e_2^2e_1 = e_1, \\ &(e_1e_2)e_2 = e_1e_2^2 = -e_1. \end{aligned} \quad (11)$$

Итак, интересующее нас множество $\mathcal{Q}_{e_1, e_2}$ является подалгеброй.

Остается проверить, что эта подалгебра изоморфна алгебре кватернионов. Для этого мы докажем, во-первых, что четверка элементов (10) образует в этой подалгебре базис, и, во-вторых, что таблица умножения для этого базиса — в точности такая же, как для базиса $1, i, j, k$ в алгебре кватернионов.

Для доказательства того, что элементы (10) составляют базис, заметим, что любой элемент подалгебры $\mathcal{Q}_{e_1, e_2}$ по ним разлагается; следовательно, остается лишь показать, что указанные элементы линейно независимы или (см. 3° § 8) что ни один из четырех элементов (10) не разлагается по *предшествующим* ему элементам этой четверки. Но элемент e_2 не разлагается

по e_1, $\mathbf{1}$ (это следует из того факта, что элементы e_1, e_2 не принадлежат одной подалгебре $\mathcal{K}_a$). Остается поэтому проверить, что e_1e_2 не разлагается по e_2, e_1, $\mathbf{1}$, т. е. что невозможно равенство вида

$$e_1e_2 = pe_2 + qe_1 + r\mathbf{1}. \tag{12}$$

Предположим, что такое соотношение имеет место. Тогда ни одно из чисел p, q не равно нулю (если бы, например, было $p = 0$, то, умножив обе части (12) слева на e_1, мы получили бы, что e_2 разлагается по e_1 и $\mathbf{1}$, что невозможно). Умножая обе части (12) слева на e_1, получим

$$-e_2 = pe_1e_2 - q\mathbf{1} + re_1$$

или

$$e_1e_2 = -\frac{1}{p}e_2 - \frac{r}{p}e_1 + \frac{q}{p}\mathbf{1}.$$

Вычитая из одного выражения для e_1e_2 другое, получим

$$\left(p + \frac{1}{p}\right)e_2 + \left(q + \frac{r}{p}\right)e_1 + \left(r - \frac{q}{p}\right)\mathbf{1} = 0.$$

В этом равенстве коэффициент при e_2 должен быть равен нулю (иначе получилось бы, что e_2 разлагается по e_1 и $\mathbf{1}$), что невозможно ни при каком действительном p.

Таким образом, элементы

$$\mathbf{1},\ e_1,\ e_2,\ e_3,$$

где $e_3 = e_1e_2$, образуют базис подалгебры $\mathcal{Q}_{e_1, e_2}$.

Чтобы установить, что подалгебра $\mathcal{Q}_{e_1, e_2}$ изоморфна алгебре $\mathcal{Q}$ кватернионов, остается сделать последний шаг: показать, что таблица умножения для алгебры $\mathcal{Q}_{e_1, e_2}$ в базисе

$$\mathbf{1},\ e_1,\ e_2,\ e_3$$

в точности такая же, как для алгебры $\mathcal{Q}$ в базисе

$$\mathbf{1},\ i,\ j,\ k.$$

Но это непосредственно видно из соотношений (5), (8), (11).

5°. Доказательство обобщенной теоремы Фробениуса, опирающееся на теорему Гурвица. Выскажем сначала некоторое замечание по поводу определения альтернативной алгебры. Мы назвали альтернативностью выполнение тождеств

$$(ab)\,b = a\,(bb) \quad \text{и} \quad b\,(ba) = (bb)\,a.$$

Однако, помимо этого определения, имеется еще и другое, которое мы будем называть вторым определением альтернативности. Оно состоит в следующем.

Пусть a и b — два произвольных элемента алгебры $\mathcal{A}$. Рассмотрим всевозможные произведения, составленные из них. Если каждое такое произведение не зависит от способа расстановки скобок, алгебра $\mathcal{A}$ называется *альтернативной*.

Например, это означает, что

$$(ab)\,b = a\,(bb),$$

$$(ab)\,(ba) = (a\,(bb))\,a$$

и т. п.

Очевидно, из второго определения альтернативности следует первое. Можно показать, что и обратно, из первого определения следует второе (этот факт составляет содержание теоремы Артина, которую мы здесь доказывать не будем).

При доказательстве обобщенной теоремы Фробениуса мы будем исходить из второго определения альтернативности. Таким образом, строго говоря, мы докажем следующую теорему: *если алгебра $\mathcal{A}$ с делением такова, что любое произведение, составленное из двух произвольных элементов a и b, не зависит от расстановки скобок, то алгебра $\mathcal{A}$ изоморфна одной из четырех алгебр: действительных чисел, комплексных чисел, кватернионов или октав.*

Важным моментом доказательства является тот факт, что утверждения I, II, III о свойствах ассоциативной алгебры с делением остаются справедливыми и в случае альтернативной алгебры с делением.

Что касается утверждений II и III, то в их доказательствах, приведенных выше, не нужно менять ни строчки. Действительно, если внимательно просмотреть эти доказательства, то обнаружится, что ассоциативность алгебры используется только в двух местах: в формуле $a^n \cdot a^m = a^{n+m}$ для перемножения степеней и в соотношении $(e_1e_2)(e_2e_1) = (e_1e_2^2)e_1$, примененном в цепочке равенств (9). Но очевидно, и то и другое остается справедливым в случае альтернативной алгебры.

Доказательство утверждения I для альтернативного случая придется несколько изменить. Найдя элемент e из уравнения $xa = a$ и умножив обе части равенства $ea = a$ слева на e, получим $e\,(ea) = ea$ или, учитывая альтернативность, $(ee)\,a = ea$. Отсюда следует, что $ee = e$. Опять-таки в силу альтернативности имеем $(be)\,e = b\,(ee)$ и $e\,(ec) = (ee)\,c$, т. е. $(be)\,e = be$ и $e\,(ec) = ec$. Отсюда следует $be = b$ и $ec = c$. Значит, e — единица алгебры.

Чтобы теперь доказать обобщенную теорему Фробениуса, можно было бы пойти по тому же пути, что и при доказательстве теоремы Фробениуса, т. е. показать, что если рассматриваемая нами альтернативная алгебра $\mathcal{A}$ не исчерпывается подалгеброй $\mathcal{Q}_{a,\,b}$, то в ней содержится подалгебра, изоморфная алгебре октав; после чего оставалось бы только доказать, что эта подалгебра совпадает со всей алгеброй $\mathcal{A}$. Такой способ доказательства возможен, однако он потребовал бы довольно длинных рассуждений. Поэтому мы выберем другой путь, а именно, попытаемся доказать, что алгебра $\mathcal{A}$ является нормированной. Отсюда по теореме Гурвица будет следовать нужный нам результат.

Введем в алгебре $\mathscr{A}$ операцию сопряжения следующим образом. Если элемент a пропорционален 1, то $\overline{a} = a$. Если же a не пропорционален 1, то, согласно утверждению II, он содержится в комплексной подалгебре $\mathscr{K}_a$. В этой подалгебре для элемента a имеется сопряженный элемент $\overline{a}$, который мы и примем за элемент, сопряженный к a в алгебре $\mathscr{A}$.

Из определения $\overline{a}$ непосредственно вытекает, что $\overline{\overline{a}} = a$, а также

$$\overline{ka} = k\overline{a}, \tag{13}$$

где k — любое действительное число.

Для вывода других свойств сопряжения нам необходимо выяснить один вопрос. Пусть элемент a не пропорционален 1. Рассмотрим какую-либо кватернионную подалгебру $\mathscr{Q}_{a_1, a_2}$, содержащую a. В этой подалгебре для a тоже имеется сопряженный элемент $\widetilde{a}$. Будет ли он совпадать с определенным выше элементом $\overline{a}$? Покажем, что будет.

Элементы a и $\overline{a}$, как сопряженные в комплексной алгебре, удовлетворяют условиям

$$a + \overline{a} = (\text{действительное число}) \cdot 1 \tag{14}$$

и

$$a\overline{a} = (\text{действительное число}) \cdot 1. \tag{15}$$

Элементы a и $\widetilde{a}$ как сопряженные в алгебре кватернионов удовлетворяют аналогичным условиям:

$$a + \widetilde{a} = (\text{действительное число}) \cdot 1 \tag{14'}$$

и

$$a\widetilde{a} = (\text{действительное число}) \cdot 1. \tag{15'}$$

Вычитая из равенств (14) и (15) соответственно равенства (14') и (15'), получим

$$\overline{a} - \widetilde{a} = (\text{действительное число}) \cdot 1$$

и

$$a(\overline{a} - \widetilde{a}) = (\text{действительное число}) \cdot 1.$$

Если $\overline{a} \neq \widetilde{a}$, то из этих соотношений вытекает, что элемент a пропорционален 1, что противоречит предположению.

Таким образом, *элемент, сопряженный a, один и тот же, независимо от того, рассматриваем ли мы a как элемент комплексной подалгебры* $\mathscr{K}_a$ (т. е. как комплексное число) *или же как элемент какой-либо подалгебры* $\mathscr{Q}_{a_1, a_2}$ (т. е. как кватернион).

Заметим попутно, что то же самое относится и к *модулю* элемента a. Поскольку $(\text{модуль } a)^2 = a\overline{a}$ как в случае комплексных чисел, так и в случае кватернионов, то модуль элемента a не зависит от того, рассматриваем ли мы a как элемент комплексной или же кватернионной подалгебры.

Из того, что доказано нами относительно сопряжения, легко следует, что для любых двух элементов a и b алгебры $\mathscr{A}$

справедливы равенства

$$\overline{a+b}=\overline{a}+\overline{b}, \tag{16}$$

$$\overline{ab}=\overline{b}\,\overline{a}. \tag{17}$$

Действительно, если a и b принадлежат одной комплексной подалгебре (т. е. $\mathscr{K}_a$ совпадает с $\mathscr{K}_b$), то написанные равенства суть свойства сопряжения в этой подалгебре; если же b не содержится в $\mathscr{K}_a$, то эти равенства снова справедливы — уже как свойства сопряжения в $\mathscr{Q}_{a,\,b}$.

Из формулы (17) и из $\overline{\overline{b}}=b$ вытекает, что элемент, сопряженный $a\overline{b}$, равен $b\overline{a}$; следовательно,

$$a\overline{b}+b\overline{a}=(\text{действительное число})\cdot 1.$$

Определим в алгебре $\mathscr{A}$ скалярное произведение (a, b) с помощью формулы

$$a\overline{b}+b\overline{a}=2(a, b)\cdot 1.$$

Что выражение (a, b) обладает всеми свойствами скалярного произведения, проверяется просто. Напомним эти свойства:

1) $(a, a)>0$, если $a\neq 0$, и $(0, 0)=0$;

2) $(a, b)=(b, a)$;

3) $(a, kb)=k(a, b)$;

4) $(a, b_1+b_2)=(a, b_1)+(a, b_2)$.

В данном случае свойство 2) очевидно. Свойства 3) и 4) вытекают непосредственно из формул (13) и (16). Для доказательства свойства 1) следует написать

$$(a, a)\cdot 1=a\overline{a}=(\text{модуль } a)^2\cdot 1 \tag{18}$$

и учесть, что модуль комплексного числа a строго положителен, если $a\neq 0$, и равен нулю, если $a=0$.

Заметим, что из равенств (18) следует

$$\sqrt{(a, a)}=\text{модуль } a,$$

т. е. норма элемента a в алгебре $\mathscr{A}$ совпадает с модулем a как комплексного числа (или кватерниона).

Так как любые два элемента a и b алгебры $\mathscr{A}$ принадлежат одной комплексной или одной кватернионной подалгебре, то

$$(\text{модуль } ab)^2=(\text{модуль } a)^2\cdot(\text{модуль } b)^2$$

(ведь алгебра комплексных чисел, так же как и алгебра кватернионов, является нормированной), или

$$(ab, ab)=(a, a)(b, b).$$

Но это равенство как раз и означает нормированность алгебры $\mathscr{A}$. Дальше вступает в действие теорема Гурвица, согласно которой алгебра $\mathscr{A}$ изоморфна одной из четырех «стандартных» алгебр: действительных чисел, комплексных чисел, кватернионов, октав. В этом как раз и заключается обобщенная теорема Фробениуса.

§ 20. Коммутативные алгебры с делением

1°. **Формулировка результата.** В предыдущем параграфе мы нашли все алгебры с делением, удовлетворяющие дополнительно условию ассоциативности. Ниже будет дано описание всех алгебр с делением при дополнительном условии *коммутативности*.

Прежде всего сошлемся на следующий факт, которого мы доказывать здесь не будем.

Любая коммутативная алгебра с делением имеет размерность не выше 2 *).

Поэтому для решения поставленной задачи нам остается перечислить все коммутативные алгебры с делением размерности 2.

Чтобы сформулировать ответ, введем обозначение $\mathcal{A}(\alpha, \beta, \gamma)$ для коммутативной алгебры размерности 2 с таблицей умножения вида

$$\begin{aligned} k_1 \circ k_1 &= \alpha k_1 + \beta k_2, \\ k_2 \circ k_2 &= -\alpha k_1 - \beta k_2, \\ k_1 \circ k_2 &= \beta k_1 + \gamma k_2, \end{aligned} \tag{1}$$

где числа α, β, γ удовлетворяют следующим условиям:

1) $\alpha\gamma - \beta^2 = \pm 1$;

2) $\beta \geqslant 0$;

3) $\alpha \geqslant 0$, причем если $\alpha = 0$, то $\gamma \geqslant 0$.

Теорема. *Любая коммутативная алгебра $\mathcal{A}$ с делением размерности 2 изоморфна одной из алгебр $\mathcal{A}(\alpha, \beta, \gamma)$. Все алгебры $\mathcal{A}(\alpha, \beta, \gamma)$ суть алгебры с делением и никакие две из них не изоморфны друг другу.*

Дальнейшая часть параграфа посвящена доказательству этой теоремы.

---

*) Остроумное доказательство этого предложения, использующее топологические соображения, нам сообщил Г. Шпиз. Приведем это доказательство для читателя, знакомого с элементарными понятиями топологии.

Пусть $\mathcal{A}$ — коммутативная алгебра с делением размерности n. Если для каких-нибудь двух элементов x и y справедливо равенство $x^2 = y^2$, то в силу коммутативности имеем $(x-y)(x+y) = 0$; ввиду отсутствия делителей нуля это означает $x = y$ или $x = -y$. Отсюда видно, что отображение $x \to x^2$ индуцирует мономорфное и непрерывное отображение сферы S^{n-1} в проективное пространство RP^{n-1}. Как известно, такое отображение возможно только при $n = 2$.

2°. Связь между операцией умножения в алгебре $\mathscr{A}$ и умножением комплексных чисел. Итак, пусть $\mathscr{A}$ — коммутативная алгебра с делением. Обозначим умножение в алгебре $\mathscr{A}$ через $x \square y$.

Зафиксируем какой-нибудь элемент $a \neq 0$ и рассмотрим преобразование $x \to a \square x$. Это преобразование является, очевидно, линейным. Обозначим его A. Так как данная алгебра есть алгебра с делением, то для преобразования A существует обратное преобразование A^{-1}.

Введем для элементов нашей алгебры новый закон умножения

$$x \cdot y = A^{-1}(x) \square A^{-1}(y). \tag{2}$$

Алгебра с умножением $x \cdot y$ снова является алгеброй с делением (из однозначной разрешимости уравнений $a \square x = b$ и $x \square a = b$ вытекает однозначная разрешимость уравнений $a \cdot x = b$ и $x \cdot a = b$). В этой алгебре элемент $a \square a$ играет роль единицы (доказательство см. на стр. 111, где рассматривается аналогичная конструкция). Но единственная алгебра с делением, обладающая единицей, — это алгебра комплексных чисел (§ 2). Поэтому элементы x и y можно трактовать как комплексные числа, а операцию $x \cdot y$ как обычное умножение комплексных чисел.

Обозначая $A^{-1}(x)$ через u и $A^{-1}(y)$ через v, перепишем (2) в виде

$$u \square v = A(u) \cdot A(v).$$

Тем самым умножение в исходной алгебре $\mathscr{A}$ мы выразили через умножение в алгебре комплексных чисел.

Сделаем теперь следующий шаг: рассмотрим умножение

$$u \circ v = A(u \cdot v) \tag{3}$$

и покажем, что алгебры с умножениями $u \square v$ и $u \circ v$ изоморфны.

Для этого запишем таблицу умножения $\circ$ в какомнибудь базисе e_1, e_2 и докажем, что она в точности совпадает с таблицей умножения $\square$ в базисе $e_1' = A^{-1}(e_1)$, $e_2' = A^{-1}(e_2)$.

Действительно, пусть

$$e_i \circ e_j = \alpha e_1 + \beta e_2.$$

Тогда

$$e'_i \square e'_j = A(e'_i) \cdot A(e'_j) = e_i \cdot e_j = A^{-1}(e_i \circ e_j) =$$
$$= A^{-1}(\alpha e_1 + \beta e_2) = \alpha A^{-1}(e_1) + \beta A^{-1}(e_2) = \alpha e'_1 + \beta e'_2,$$

что и доказывает совпадение таблиц умножения.

Итак, мы показали, что исходная алгебра $\mathscr{A}$ изоморфна алгебре с умножением (3), где $u \cdot v$ есть обычное произведение комплексных чисел, а A — некоторое линейное преобразование, для которого существует обратное преобразование A^{-1}. С другой стороны, очевидно, что любая алгебра такого рода есть коммутативная алгебра с делением. Таким образом, задача перечисления всех алгебр с делением размерности 2 свелась к тому, чтобы среди алгебр (3) выделить все неизоморфные между собой.

3°. Отыскание алгебры $\mathscr{A}(\alpha, \beta, \gamma)$, изоморфной алгебре $\mathscr{A}$. Нам необходимо в алгебре (3) найти такой базис k_1, k_2, в котором таблица умножения имеет вид (1) (с некоторыми ограничениями на α, β, γ). Запишем сначала таблицу умножения алгебры (3) в базисе

$$e_1 = 1, \quad e_2 = i.$$

Поскольку

$$e_1 \circ e_1 = A(e_1 \cdot e_1) = A(1),$$
$$e_2 \circ e_2 = A(e_2 \cdot e_2) = A(-1) = -A(1),$$
$$e_1 \circ e_2 = A(e_1 \cdot e_2) = A(i),$$

то, полагая $A(1) = a + bi$, $A(i) = c + di$, будем иметь

$$\begin{aligned} e_1 \circ e_1 &= ae_1 + be_2, \\ e_2 \circ e_2 &= -ae_1 - be_2, \\ e_1 \circ e_2 &= ce_1 + de_2. \end{aligned} \tag{4}$$

Поставим вопрос: существуют ли, помимо e_1, e_2 (т. е. помимо 1, i), в алгебре $\mathscr{A}$ другие базисы, в которых таблица умножения подобна таблице (4):

$$\begin{aligned} k_1 \circ k_1 &= \alpha k_1 + \beta k_2, \\ k_2 \circ k_2 &= -\alpha k_1 - \beta k_2, \\ k_1 \circ k_2 &= \delta k_1 + \gamma k_2; \end{aligned} \tag{5}$$

иначе говоря, существуют ли базисы, для которых

$$k_1 \circ k_1 = -k_2 \circ k_2. \tag{6}$$

Так как равенство (6) равнозначно $A(k_1 \cdot k_1) = -A(k_2 \cdot k_2)$ или $A(k_1 \cdot k_1) = A(-k_2 \cdot k_2)$, то из существования обратного преобразования A^{-1} следует, что $k_1 \cdot k_1 = -k_2 \cdot k_2$, или

$$k_2 = \pm ik_1.$$

Следовательно, *все базисы, в которых таблица умножения имеет вид* (5), *суть*

$$k_1 = f, \quad k_2 = \pm if, \tag{7}$$

где f *— произвольное* (*не равное нулю*) *комплексное число.*

Базисов (7), разумеется, существует бесчисленное множество. Сейчас мы покажем, что среди них обязательно найдется такой, в котором выполняется условие

$$\beta = \delta,$$

т. е. базис, в котором таблица умножения имеет вид (1).

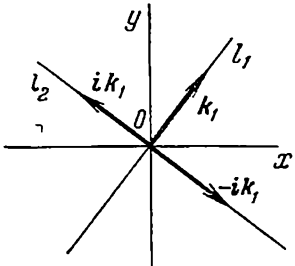


Рис. 17.

Для этой цели примем снова за исходный базис $e_1 = 1$, $e_2 = i$, а искомый базис запишем в виде

$$k_1 = \rho(\cos\varphi + i\sin\varphi),$$
$$k_2 = \pm i\rho(\cos\varphi + i\sin\varphi).$$

Чтобы отыскать ρ и φ, мы должны:

a) вычислить произведение $k_1 \circ k_1$, исходя из формул (4), и полученный элемент разложить по k_1 и k_2;

b) вычислить таким же образом произведение $k_1 \circ k_2$ и полученный элемент разложить по k_1 и k_2;

c) коэффициент при k_2 в первом разложении приравнять коэффициенту при k_1 во втором разложении.

Эту вычислительную работу мы предоставляем сделать читателю. Результат будет следующим: на ρ не накладывается никаких ограничений, а φ находится из условия

$$\operatorname{tg}\varphi = \frac{b-c}{a+d}.$$

Очевидно, это условие определяет угол φ с точностью до слагаемого вида πn и, значит, определяет на плоскости два луча (рис. 17), составляющих одну прямую l_1. На этой прямой лежит вектор, изображающий ком-

плексное число k_1 (или, как мы будем говорить, вектор k_1). Другой вектор $k_2 = \pm ik_1$ лежит на своей прямой l_2. Длины обоих векторов совпадают.

Итак, приходим к следующему описанию всех базисов k_1, k_2, в которых таблица умножения имеет вид (1). Базисный вектор k_1 выбирается на однозначно определяемой прямой l_1, базисный вектор k_2 — на перпендикулярной прямой l_2; длины ρ векторов должны быть одинаковы. Заметим, что при данной длине возможны ровно 4 искомых базиса (рис. 18).

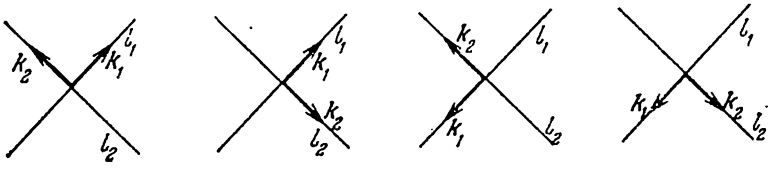


Рис. 18.

Теперь следует сказать, что если от базиса k_1, k_2 мы переходим к другому базису λk_1, λk_2, где λ — положительное действительное число, то все коэффициенты в таблице умножения (1) умножаются на λ. Поэтому, если наложить на базис дополнительное условие

$$\alpha\gamma - \beta^2 = \pm 1,$$

то этим самым определится единственное значение λ. Тогда от указанного выше бесчисленного множества базисов останутся ровно 4 базиса (см. рис. 18).

Итак, существуют ровно 4 базиса:

$$k_1 = \pm k, \quad k_2 = \pm ik,$$

для которых таблица умножения имеет вид

$$\begin{aligned} k_1 \circ k_1 &= \alpha k_1 + \beta k_2, \\ k_2 \circ k_2 &= -\alpha k_1 - \beta k_2, \\ k_1 \circ k_2 &= \beta k_1 + \gamma k_2, \end{aligned} \tag{1}$$

причем

$$\alpha\gamma - \beta^2 = \pm 1.$$

Сделаем теперь последний шаг: покажем, что среди указанных выше четырех базисов можно выбрать такой, в котором $\beta \geqslant 0$ и $\alpha \geqslant 0$, причем если $\alpha = 0$, то $\gamma \geqslant 0$.

Действительно, если в базисе k_1, k_2 имеем $\beta < 0$, то, перейдя к базису k_1, $-k_2$, получим новую таблицу, в которой $\beta > 0$. Аналогично, если $\alpha < 0$, то, умножив первый базисный вектор на -1, получим таблицу, в которой $\alpha > 0$ (при этом знак β не меняется); если же $\alpha = 0$, то это же преобразование позволяет изменить знак γ.

Подведем итог. Для каждой коммутативной алгебры $\mathscr{A}$ с делением размерности 2 существует базис, в котором таблица умножения имеет вид (1), где

1) $\alpha\gamma - \beta^2 = \pm 1$,

2) $\beta \geqslant 0$,

3) $\alpha \geqslant 0$, причем если $\alpha = 0$, то $\gamma \geqslant 0$.

Этот базис, вообще говоря, единствен; в некоторых особенных случаях (когда $\beta = 0$ или $\alpha = \gamma = 0$) таких базисов будет два, но таблица (1) для них будет одна и та же.

Отсюда видно, что каждой алгебре $\mathscr{A}$ отвечает единственная таблица (1) с указанными выше ограничениями на α, β, γ, т. е. алгебра $\mathscr{A}$ *изоморфна одной и только одной алгебре* $\mathscr{A}(\alpha, \beta, \gamma)$.

То, что любая алгебра $\mathscr{A}(\alpha, \beta, \gamma)$ является алгеброй с делением, следует хотя бы из того факта, что каждая такая алгебра имеет вид

$$u \circ v = A(u \cdot v),$$

где преобразование A действует по формулам

$$A(k_1) = \alpha k_1 + \beta k_2,$$
$$A(k_2) = \beta k_1 + \gamma k_2,$$

причем $\alpha\gamma - \beta^2 \neq 0$. В самом деле, из условия $\frac{\alpha}{\beta} \neq \frac{\beta}{\gamma}$ (эквивалентного $\alpha\gamma - \beta^2 \neq 0$) вытекает, что $A(k_1) \neq \neq \lambda A(k_2)$ и тем самым что векторы $A(k_1)$ и $A(k_2)$ образуют базис. Отсюда нетрудно получить, что для преобразования A существует обратное преобразование A^{-1}, а отсюда, в свою очередь — что алгебра с умножением $u \circ v$ есть алгебра с делением. Теорема доказана.

ЗАКЛЮЧЕНИЕ

Бóльшая часть того, о чем говорилось в этой книжке, относится к первоначальному этапу в развитии теории алгебр. Мы хотим теперь рассказать, хотя и очень бегло, о некоторых дальнейших результатах этой теории.

Развитие теории алгебр начинается с работы В. Гамильтона о кватернионах, напечатанной в 1843 г. Позднее ее содержание вместе с рядом других результатов было им подробно изложено в «Лекциях о кватернионах». Влияние идей Гамильтона было весьма значительным: они подготовили почву для целой серии работ об ассоциативных алгебрах, завершившейся доказательством ряда глубоких теорем о строении таких алгебр.

Чтобы рассказать об этих теоремах, уточним сначала один существенный момент, которого до сих пор мы совсем не касались. Он связан с величинами $a_1, a_2, \ldots, a_n$, являющимися коэффициентами в выражении

$$a_1 i_1 + a_2 i_2 + \ldots + a_n i_n \qquad (1)$$

для элементов n-мерной алгебры. В нашем изложении эти величины всегда предполагались действительными числами. В этом случае принято на самом деле говорить об *алгебрах над полем действительных чисел*. Наряду с ними приходится рассматривать и другие алгебры, элементы которых представляют собой выражения вида (1), где $a_1, a_2, \ldots, a_n$ — произвольные комплексные числа; такие алгебры называются *алгебрами над полем комплексных чисел*. Кроме поля действительных и поля

комплексных чисел, имеется много других полей*) (например, поле рациональных чисел) и соответственно этому много других типов алгебр.

Многие результаты в теории алгебр очень сильно меняются в зависимости от того, какому полю принадлежат коэффициенты $a_1, \ldots, a_n$ в выражениях (1), т. е. над каким полем рассматриваются алгебры. Например, над полем действительных чисел существуют, как мы знаем, три ассоциативные алгебры с делением (и бесконечное множество неассоциативных алгебр такого рода), и в то же время имеется *только одна комплексная алгебра с делением*. Это — одномерная алгебра, состоящая из самых комплексных чисел. Кроме нее не существует ни одной алгебры с делением над полем комплексных чисел (даже без условия ассоциативности). Доказательство этого факта несложно, но мы на нем не останавливаемся.

Введем теперь такие определения.

1. *Идеалом* алгебры $\mathscr{A}$ называется такое подпространство $\mathscr{U}$, что

$$\mathscr{A}\mathscr{U} \subset \mathscr{U} \quad \text{и} \quad \mathscr{U}\mathscr{A} \subset \mathscr{U}.$$

Это означает, что, каковы бы ни были элементы $a \in \mathscr{A}$ и $u \in \mathscr{U}$, оба произведения au и ua принадлежат $\mathscr{U}$. Иначе говоря, произведение элемента, взятого из идеала, на любой элемент алгебры снова принадлежит идеалу.

При этом два крайних случая — когда подпространство $\mathscr{U}$ совпадает со всей алгеброй $\mathscr{A}$ и когда $\mathscr{U}$ состоит из единственного элемента 0 — не принято рассматривать как идеалы (впрочем, иногда говорят, что $\mathscr{A}$ и 0 являются несобственными идеалами).

---

*) Общее определение поля таково. Пусть $\mathscr{P}$ — некоторое множество объектов, над которыми можно производить две операции; одну из них условно назовем *сложением* и будем обозначать $a + b$, другую назовем *умножением* и обозначим $a \cdot b$. Множество $\mathscr{P}$ называется *полем*, если обе заданные в нем операции коммутативны, ассоциативны, справедлив распределительный закон, а также выполнимо вычитание (иначе говоря, однозначно разрешимо уравнение $a + x = b$) и выполнимо деление. Последнее означает, что однозначно разрешимо уравнение $ax = b$, если $a \neq 0$; здесь 0 обозначает элемент множества $\mathscr{P}$ такой, что $a + 0 = a$ для всех $a \in \mathscr{P}$ (существование такого элемента нетрудно доказать).

Под словом «операция» в этом определении подразумевается любое правило, ставящее каждым двум элементам $a \in \mathscr{P}$ и $b \in \mathscr{P}$ в соответствие третий элемент $c \in \mathscr{P}$.

Примером идеала может служить подпространство элементов вида $b\Omega$ в алгебре дуальных чисел (т. е. чисел $a + b\Omega$, где $\Omega^2 = 0$). Другой пример — подпространство элементов вида $a(1 + E)$ в алгебре двойных чисел (чисел $a + bE$, где $E^2 = 1$).

2. Алгебра, не имеющая идеалов, называется *простой*.

Можно сказать, что понятие простой алгебры обобщает понятие алгебры с делением. Каждая алгебра с делением обязательно является простой: действительно, если у алгебры есть идеал $\mathcal{U}$, то уравнение

$$ux = b,$$

где u принадлежит идеалу, а b не принадлежит ему, не имеет решения, поэтому такая алгебра не может быть алгеброй с делением.

В конце XIX века исследования, касавшиеся теории алгебр, были сосредоточены в основном на изучении ассоциативных алгебр (как мы уже отмечали, сам термин «алгебра» фактически понимался как «ассоциативная алгебра»). В результате возникло довольно ясное представление о строении ассоциативной алгебры. Первый существенный результат относился к простым алгебрам и был получен в 1893 г. Ф. Молином; независимо тот же результат получили Г. Фробениус и Э. Картан. Оказалось, что все простые комплексные ассоциативные алгебры с точностью до изоморфизма — это полные матричные алгебры произвольного порядка n (т. е. алгебры всех квадратных матриц порядка n).

Более общую теорему, справедливую для алгебр над произвольным полем $\mathcal{P}$, доказал в 1907 г. американский математик Д. Ведерберн: *все простые ассоциативные алгебры над полем $\mathcal{P}$ — это в точности все полные матричные алгебры с элементами из ассоциативной алгебры с делением над $\mathcal{P}$.*

Например, согласно этой теореме все простые ассоциативные алгебры над полем $\mathcal{D}$ действительных чисел состоят из трех серий:

1) алгебры матриц с элементами — действительными числами;

2) алгебры матриц с элементами — комплексными числами (подчеркнем, что эти алгебры следует рассматривать как алгебры над полем $\mathcal{D}$), частным случаем (при $n = 1$) является сама алгебра комплексных чисел —

размерность ее равна 2; подобно этому алгебра всех комплексных матриц порядка n имеет размерность $2n^2$;

3) алгебры матриц с элементами — кватернионами (для матриц порядка n размерность такой алгебры равна $4n^2$).

Предыдущая теорема о комплексных простых алгебрах легко получается из теоремы Ведерберна, если вспомнить, что единственная комплексная алгебра с делением — это алгебра самих комплексных чисел.

Таким образом, все простые ассоциативные алгебры были найдены. Одновременно с этим было выяснено (теми же авторами), что структура простых ассоциативных алгебр во многом определяет строение произвольных ассоциативных алгебр. Чтобы точно сформулировать последнее утверждение, нам понадобится еще несколько определений.

3. Пусть $\mathcal{U}_1$ и $\mathcal{U}_2$ — две алгебры. Их *прямой суммой* называется новая алгебра $\mathcal{A}$, элементы которой суть всевозможные пары

$$(u_1, u_2) \quad (\text{где } u_1 \in \mathcal{U}_1,\ u_2 \in \mathcal{U}_2)$$

со следующими законами сложения и умножения:

$$(u_1, u_2) + (u_1', u_2') = (u_1 + u_1',\ u_2 + u_2'),$$
$$(u_1, u_2) \cdot (u_1', u_2') = (u_1 u_1',\ u_2 u_2').$$

Легко видеть, что элементы вида $(u_1, 0)$ образуют подалгебру алгебры $\mathcal{A}$, причем эта подалгебра изоморфна $\mathcal{U}_1$; обозначим ее $\mathcal{A}_1$. Аналогично элементы вида $(0, u_2)$ образуют подалгебру $\mathcal{A}_2$, изоморфную $\mathcal{U}_2$. Обе указанные подалгебры являются идеалами; например, для первой из них это следует из равенств

$$(u_1, 0)(u_1', u_2') = (u_1 u_1', 0), \quad (u_1', u_2')(u_1, 0) = (u_1' u_1, 0).$$

Заметим, что подалгебры $\mathcal{A}_1$ и $\mathcal{A}_2$ являются *взаимно дополнительными*: так мы называем две подалгебры, обладающие тем свойством, что любой элемент алгебры представляется, и притом единственным образом, в виде $a_1 + a_2$, где $a_1 \in \mathcal{A}_1$, $a_2 \in \mathcal{A}_2$.

Аналогично прямой сумме двух алгебр определяется прямая сумма любого числа алгебр. Элементами прямой суммы алгебр $\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_k$ являются всевозможные наборы

$$(u_1, u_2, \ldots, u_k) \qquad (\text{где } u_1 \in \mathcal{U}_1, \ldots, u_k \in \mathcal{U}_k).$$

Примером прямой суммы является алгебра матриц порядка $p+q$, имеющих «блочно-диагональный» вид

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right),$$

где A и B — произвольные матрицы порядков p и q соответственно. Нетрудно проверить, что для произведения таких матриц справедлива формула

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)\left(\begin{array}{c|c} A' & 0 \\ \hline 0 & B' \end{array}\right)=\left(\begin{array}{c|c} AA' & 0 \\ \hline 0 & BB' \end{array}\right),$$

откуда видно, что данная алгебра изоморфна прямой сумме алгебры всех матриц порядка p и алгебры всех матриц порядка q.

Интересно отметить, что рассмотренная нами в начале книги (см. § 2) алгебра двойных чисел изоморфна прямой сумме двух алгебр действительных чисел. В самом деле, выберем в качестве базиса следующие два элемента алгебры $\mathscr{A}$:

$$i_1=\frac{1-E}{\sqrt{2}}, \quad i_2=\frac{1+E}{\sqrt{2}}.$$

Очевидно,

$$i_1^2=i_1, \quad i_2^2=i_2, \quad i_1i_2=0.$$

Каждый элемент $a\in\mathscr{A}$ можно однозначно представить в виде суммы

$$a_1i_1+a_2i_2,$$

причем для произведения двух элементов справедлива формула

$$(a_1i_1+a_2i_2)(b_1i_1+b_2i_2)=a_1b_1i_1+a_2b_2i_2.$$

Ставя в соответствие элементу a пару чисел (a_1, a_2), мы видим отсюда, что алгебра $\mathscr{A}$ есть прямая сумма двух алгебр $\mathscr{D}$ (действительных чисел).

4. *Полупростой* алгеброй называется прямая сумма простых.

Так как прямая сумма однозначно определяется своими слагаемыми, то все полупростые ассоциативные алгебры можно считать известными, коль скоро известны все простые ассоциативные алгебры.

Например, любая полупростая ассоциативная алгебра над полем комплексных чисел изоморфна алгебре

всех «блочно-диагональных» матриц с блоками порядков $p_1, p_2, \ldots, p_k$ по диагонали (числа $p_1, p_2, \ldots, p_k$ фиксированы). В частности, при $k = 3$ получаем матрицы вида

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline 0 & B & 0 \\ \hline 0 & 0 & C \end{array}\right).$$

5. Алгебра называется *нильпотентной*, если существует такое число k, что произведение любых k элементов равно нулю, причем скобки в произведении расставлены произвольно. (Мы привели определение нильпотентной алгебры в общем случае, т. е. без условия ассоциативности. Поэтому необходимо последнее добавление о произвольном порядке перемножения.)

Подалгебра некоторой алгебры называется *нильпотентной*, если она, рассматриваемая как самостоятельная алгебра, является нильпотентной.

Простейшим примером нильпотентной алгебры является нулевая алгебра (произведение любых двух элементов равно нулю). Другой пример — алгебра с базисом i_1, i_2, i_3 и таблицей умножения

$$\begin{cases} i_1 i_2 = i_3, \\ \text{остальные } i_\alpha i_\beta \text{ равны } 0. \end{cases}$$

Заметим, что нильпотентные алгебры в некотором смысле противоположны по своим свойствам полупростым алгебрам. Например, для нильпотентной алгебры $\mathscr{A}$ некоторая «степень» $\mathscr{A}^k$, т. е. множество произведений каких угодно k элементов алгебры $\mathscr{A}$, состоит из одного нуля (в этом и заключается определение нильпотентной алгебры); между тем в случае полупростой алгебры любая степень совпадает со всей алгеброй.

Нетрудно доказать, что если $\mathscr{V}_1$ и $\mathscr{V}_2$ — два нильпотентных идеала произвольной алгебры $\mathscr{A}$, то их сумма (т. е. совокупность элементов вида $v_1 + v_2$, где $v_1 \in \mathscr{V}_1$, $v_2 \in \mathscr{V}_2$) есть снова нильпотентный идеал. Отсюда легко вывести, что среди всех нильпотентных идеалов алгебры $\mathscr{A}$ существует *максимальный*, т. е. такой, который содержит все другие нильпотентные идеалы.

Теперь мы можем сформулировать основную теорему в теории ассоциативных алгебр.

Теорема Ведерберна. *В произвольной ассоциативной алгебре $\mathscr{A}$ существует полупростая подалгебра $\mathscr{U}$, дополнительная к максимальному нильпотентному идеалу $\mathscr{V}$.*

Другими словами, каждый элемент $a \in \mathscr{A}$ однозначно представляется в виде суммы $u + v$, где первое слагаемое принадлежит полупростой подалгебре $\mathscr{U}$, а второе — максимальному нильпотентному идеалу $\mathscr{V}$; тем самым элементу a однозначно сопоставляется пара (u, v), где $u \in \mathscr{U}$, $v \in \mathscr{V}$. При этом для произведения любых двух элементов алгебры $\mathscr{A}$ справедлива формула

$$(u_1, v_1)(u_2, v_2) = (u_1u_2, v), \tag{2}$$

где $v = u_1v_2 + v_1u_2 + v_1v_2 \in \mathscr{V}$ (следует учесть, что $\mathscr{V}$ — идеал).

В частном случае, когда подалгебра $\mathscr{U}$ тоже является идеалом, каждое из произведений u_1v_2 и v_1u_2 равно 0 (так как оно должно принадлежать одновременно $\mathscr{U}$ и $\mathscr{V}$), и формула для умножения принимает вид

$$(u_1, v_1)(u_2, v_2) = (u_1u_2, v_1v_2).$$

В этом случае алгебра $\mathscr{A}$ является прямым произведением алгебр $\mathscr{U}$ и $\mathscr{V}$. В общем же случае строение алгебры $\mathscr{A}$ не определяется целиком строением алгебр $\mathscr{U}$ и $\mathscr{V}$ по отдельности, так как элемент v в (2) зависит не только от v_1, v_2, но еще и от u_1, u_2. Однако все же то обстоятельство, что любую ассоциативную алгебру $\mathscr{A}$ можно представить множеством пар (u, v), где u пробегает некоторую полупростую алгебру, а v — нильпотентную, причем умножение подчиняется закону (2), сильно проясняет строение ассоциативных алгебр.

В качестве примера к теореме Ведерберна рассмотрим алгебру матриц порядка $p+q$, у которых элементы последних q строчек суть нули. Любую такую матрицу можно записать в виде

$$\left(\begin{array}{c|c} u & v \\ \hline 0 & 0 \end{array}\right), \tag{3}$$

где u обозначает квадратную матрицу порядка p, а v — прямоугольную матрицу с p строками и q столбцами. Нетрудно показать, что максимальный нильпотентный идеал $\mathscr{V}$ состоит из матриц (3) при $u = 0$ (и является нулевой алгеброй); в качестве дополнительной к нему полупростой подалгебры $\mathscr{U}$ можно взять множество

матриц (3) при $v = 0$ (в данном случае подалгебра $\mathcal{U}$ является простой).

Чтобы подчеркнуть содержательность теоремы Ведерберна, приведем примеры двумерных алгебр (естественно, не ассоциативных), для которых утверждение теоремы неверно.

В первом примере таблица умножения имеет вид

$$e_1e_1 = e_1 + e_2, \quad e_2e_2 = 0, \quad e_1e_2 = e_2, \quad e_2e_1 = 0.$$

Легко видеть, что элементы вида ke_2 образуют одномерный нильпотентный идеал $\mathcal{N}$. Этот идеал максимален, поскольку единственное содержащее его подпространство есть вся алгебра, а она не является нильпотентной (любая степень элемента e_1 отлична от нуля). Легко проверить, что, кроме $\mathcal{N}$, не существует других подалгебр данной алгебры; тем самым не существует и дополнительной подалгебры к $\mathcal{N}$.

Вторая алгебра имеет такую таблицу умножения:

$$e_1e_1 = e_1, \quad e_2e_2 = e_2, \quad e_1e_2 = e_2, \quad e_2e_1 = 0.$$

В этой алгебре вообще нет нильпотентных идеалов. Если бы алгебра «удовлетворяла» теореме Ведерберна, то она была бы простой или полупростой. Первое не имеет места, так как алгебра содержит идеал, состоящий из элементов вида ke_2, второе также невозможно, потому что этот идеал — единственный.

Результаты, полученные в теории ассоциативных алгебр, послужили моделью для дальнейших исследований. Многие последующие работы состояли в доказательстве того, что утверждение теоремы Ведерберна справедливо для других классов алгебр (хотя для всех алгебр, как мы только что видели, оно не может быть верным) и в перечислении простых алгебр этих классов.

Было доказано (М. Цорн), что теорема Ведерберна обобщается на альтернативные алгебры, т. е. на более широкий класс алгебр, чем ассоциативные. Заметим, что при исследовании простых альтернативных алгебр выяснился любопытный факт. Хотя, на первый взгляд, класс таких алгебр должен быть много шире класса простых ассоциативных алгебр, на самом деле первый класс из второго получается — в случае поля комплексных чисел — добавлением только одной алгебры «комплексных» октав; в случае поля действительных чисел

добавляется несколько алгебр такого же типа, как октавы.

Укажем еще два класса алгебр, для которых справедлива теорема Ведерберна. Для этой цели возьмем любую ассоциативную алгебру $\mathscr{A}$ и на ее базе построим две новые алгебры $\mathscr{A}^+$ и $\mathscr{A}^-$, состоящие из тех же элементов, со следующими законами умножения:

в $\mathscr{A}^+$ $\quad a \square b = ab + ba,$

в $\mathscr{A}^-$ $\quad a \circ b = ab - ba.$

В алгебре $\mathscr{A}^+$ умножение коммутативно и, как нетрудно проверить, выполняется тождество

$$(b^2 \square a) \square b = b^2 \square (a \square b); \tag{3}$$

в алгебре $\mathscr{A}^-$ умножение антикоммутативно (т. е. $a \circ b = -b \circ a$) и выполняется тождество

$$a \circ (b \circ c) + b \circ (c \circ a) + c \circ (a \circ b) = 0. \tag{4}$$

Любая коммутативная алгебра, для которой справедливо (3), называется *йордановой алгеброй* (по имени немецкого физика П. Йордана); любая антикоммутативная алгебра, для которой справедливо (4), называется *алгеброй Ли*. Норвежский математик Софус Ли в конце XIX века впервые рассмотрел алгебры, названные потом его именем, в связи с теорией «непрерывных групп преобразований». В современной математике алгебры Ли играют важнейшую роль и находят приложение почти в каждом ее разделе.

Классификация простых йордановых алгебр была получена американским математиком А. Албертом; им же была доказана справедливость теоремы Ведерберна для йордановых алгебр.

Основные теоремы о структуре алгебр Ли были получены одним из крупнейших математиков XX века Э. Картаном. Им была найдена в частности, классификация простых алгебр Ли. Распространение теоремы Ведерберна на алгебры Ли получил Э. Леви; при этом понятие нильпотентного идеала оказалось нужным заменить на более широкое понятие *разрешимого* идеала. Рамки данной книжки не позволяют нам останавливаться подробнее на этих вопросах.

ОГЛАВЛЕНИЕ